Resumen de novedades del nuevo Reglamento general de protección de datos.

A continuación, le hacemos un breve resumen de las novedades que podrá encontrar en el nuevo reglamento general europeo de protección de datos. Este reglamenta entrará en vigor el 25 de mayo de 2018. Hasta ese momento, la legislación que está en vigor es la Ley Orgánica 15/1999 y su reglamento.

También le informamos que la Agencia Española de Protección de Datos está elaborando las directrices para el cumplimiento del reglamenta, y hasta la fecha sigue trabajando en esas directrices.

RESUMEN DE NOVEDADES.

1. La figura del Delegado de Protección de Datos.

El Reglamento impone la creación de una nueva figura llamada **Delegado de Protección de Datos (DPO, en inglés)**. Dando a los profesionales del sector una importancia fundamental en su implantación y cumplimiento.

El DPO será **obligatorio** para la **Administración Pública** y para **empresas que realicen un tratamiento de datos sistemáticamente y principalmente a gran escala** (estudios de solvencia, mercados, riesgos…) o el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 (datos relativos a creencias religiosas, preferencias políticas, salud, sexualidad, etc.…) o relativos a condenas e infracciones penales que se refiere el artículo 10.

El delegado de protección de datos tendrá como mínimo las siguientes funciones:

- **Informar y asesorar** al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones a las que se encuentran sujeto.
- **Supervisar el cumplimiento del Reglamento**, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.
- **Asesoramiento acerca de la evaluación de impacto** relativa a la protección de datos y supervisar su aplicación.

Fecha de edición:03/01/2018

- **Cooperar con la autoridad de control**, actuando como interlocutor para cuestiones relativas al tratamiento.

El delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

2. Evaluación del impacto.

La autoridad de control (en España es la Agencia Española de Protección de Datos) indicará una lista de los tipos de tratamiento que requieren una evaluación de impacto.

Esta evaluación del impacto debe ser previa cuando se considere que existe un alto riesgo debido a el tipo de datos, medios o fines para los que se realiza el tratamiento.

Debe consultarse a la autoridad de control antes de iniciar las actividades de tratamiento si una evaluación de impacto muestra que entrañaría un alto riesgo para los derechos y libertades de las personas físicas, y el responsable del tratamiento considera que el riesgo no puede mitigarse por medios razonables en cuanto a tecnología disponible y costes de aplicación.

La observación de la norma debe ser desde el diseño de productos, servicios y aplicaciones hasta su fase de desarrollo y aplicación.

3. Lugar de establecimiento del encargado del tratamiento.

El responsable o el encargado de tratamiento de datos de ciudadanos EU deben tener una dirección en la UE.

El responsable o el encargado del tratamiento no establecido en la UE que esté tratando datos personales de interesados que residan en la UE deben designar a un representante.

Como excepción, no será necesario para un tratamiento ocasional y si no incluye el tratamiento de datos especialmente protegidos o si el responsable del tratamiento es una autoridad u organismo público.

4. Códigos de conducta y certificación o sellos de marca.

Se va a promover la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos

La certificación será voluntaria y deberá tener en cuenta las características específicas de los distintos sectores y las necesidades específicas de las microempresas y las pequeñas y medianas empresas.

Los organismos de certificación que tengan un nivel adecuado de pericia en materia de protección de datos expedirán y renovarán las certificaciones una vez informada la autoridad de control (AEPD).

5. Consentimiento afirmativo para el tratamiento

El nuevo reglamento de protección de datos señala que todo tratamiento de datos personales debe ser lícito y leal.

El consentimiento para el tratamiento de los datos personales debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal (declaración por escrito, una declaración verbal, marcar una casilla, escoger parámetros técnicos para la utilización de servicios informáticos…)

El silencio, las casillas ya marcadas o la inacción no constituye consentimiento.

El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos.

6. Ejercicio de los derechos.

Se hace especial hincapié en el principio de transparencia que exige que toda información y comunicación relativa al tratamiento de los datos personales sea fácilmente accesible y fácil de entender, en resumidas cuentas, que se utilice un lenguaje sencillo y claro.

Como es hasta ahora deben quedar totalmente claros los siguientes puntos a la hora de solicitar o consultar información:

- Que se están recogiendo, utilizando, consultando o tratando datos personales.
- La medida en que dichos datos son o serán tratados.

- La identidad del responsable del tratamiento.
- Conocer los fines para los que se tratan los datos personales.
- El plazo de tratamiento.
- Los destinatarios si fuesen a cederse.
- Los derechos que les asisten de ejercitar el derecho a presentar una reclamación ante una autoridad de control.

7. Derecho al olvido.

Los interesados deben tener derecho a que se rectifiquen los datos personales que le conciernen y un "derecho al olvido"

En el entorno en online, el derecho al olvido incluye que quien publica datos personales está obligado a indicar a los responsables del tratamiento que estén tratando tales datos personales (sus fuentes) que supriman todo enlace a ellos, o las copias o réplicas de tales datos. Para entendernos, si ejerce su derecho al olvido contra Google debe ser Google quien indique a las páginas web (periódicos, foros, redes, etc..) que supriman sus datos.

8. Limitación plazo de conservación de los datos personales.

En relación plazo de conservación de los datos personales se debe garantizar que se limiten a un mínimo estricto, el responsable del tratamiento ha de establecer plazos para su supresión o revisión periódica.

9. Directrices, políticas y medidas.

Se podrán proporcionar directrices para la aplicación de medidas que denuesten el cumplimiento por parte del responsable o del encargado del tratamiento como:

- La identificación del riesgo del tratamiento en un informe previo.
- La evaluación de riesgos en términos de origen, naturaleza, probabilidad y gravedad.
- La identificación de buenas prácticas para mitigar el riesgo, como son procedimientos, certificaciones, directrices dadas por el Comité o indicaciones proporcionadas por un delegado de protección de datos.

A fin de poder demostrar la conformidad con el Reglamento, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan los principios de protección de datos desde el diseño y por defecto tales como:

- Reducir al máximo el tratamiento de datos personales
- Anonimizar lo antes posible los datos personales
- Permitir a los interesados supervisar el tratamiento de datos
- Permitir al responsable del tratamiento crear y mejorar elementos de seguridad.

10. Notificación de brechas de seguridad y exposición de los datos.

Esto es una novedad destacable. El responsable de los datos debe notificar antes de 72 horas la violación de la seguridad de los datos personales a la autoridad de control competente y, en cooperación con la autoridad de control o policiales, notificar el riesgo al interesado permitiéndole tomar las precauciones necesarias.

Si dicha notificación no es posible en el plazo de 72 horas, debe acompañarse de una indicación de los motivos.

11. Autoridades de control y Comité Europeo de Protección de Datos.

El reglamento incluye la creación de un Consejo Europeo de Protección de Datos como organismo de la Unión, que gozará de personalidad jurídica para garantizar la aplicación coherente del reglamento. Este Consejo estará formado por los representantes de cada una de las 28 autoridades de control independientes.

Las autoridades de control deben tener en todos los Estados miembros las mismas funciones y poderes efectivos, incluidos poderes de investigación, poderes correctivos y sancionadores, y poderes de autorización y consultivos.

12. No será necesario la inscripción de ficheros en la AEPD.

Otra novedad importante es la eliminación de la obligación del registro de ficheros en la AEPD.

Se deben sustituir por procedimientos y mecanismos que se centren, en los tratamientos con un alto riesgo para los derechos y libertades de las personas físicas debido al tipo de datos o las formas de tratarlos.

Los encargados o el representante del encargado, debe mantener un registro de todas las actividades y categorías de actividades de tratamiento.

Estas obligaciones no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas, a menos que el tratamiento que realice pueda entrañar un riesgo.

13. Recursos, responsabilidad y sanciones.

Se modifica de sustancialmente el régimen sancionador actual. Dispone sanciones muy severas contra los responsables o encargados del tratamiento que infrinjan las normas de protección de datos, imponiendo **multas administrativas de hasta 20.000.000 EUR o de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual** global (del grupo) del ejercicio anterior, optándose por la de mayor cuantía.

Otra novedad importante es que **el responsable o el encargado del tratamiento deberán indemnizar daños y perjuicios que pueda causar como consecuencia de un tratamiento** en infracción del Reglamento.

Las sanciones se impondrán, de forma proporcional según las circunstancias de cada caso y deben ser efectivas, proporcionadas y disuasorias.

Para las infracciones leves, o si la multa fuese una carga desproporcionada para una persona física, en lugar de sanción mediante multa **puede imponerse un apercibimiento**.