



## **GRUPO ACMS Consultores**

Nuevo reglamento sobre protección de datos



**(ER-0772/2013)**

**Alcance ISO 9001**

Diseño, desarrollo, implantación, formación y mantenimiento de sistemas de gestión de la calidad, medioambiental, de la prevención de riesgos laborales, protección de datos, seguridad alimentaria y de la calidad y competencia técnica en laboratorios clínicos.

**Alcance ISO 27001**

Los sistemas de información que dan soporte a las actividades de diseño, desarrollo, implantación, formación y mantenimiento de sistemas de gestión y el diseño, desarrollo y comercialización de software de sistemas de gestión de acuerdo con la declaración de aplicabilidad vigente.



**(SI-0021/2020)**

Publicada el 25/05/2016

## **El nuevo Reglamento Europeo sobre Protección de Datos ha entrado en vigor**

El nuevo Reglamento Europeo sobre Protección de Datos ha entrado en vigor el 25 de mayo de 2016, y será de aplicación en todos los Estados de la UE a partir del 25 de mayo de 2018.

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.

El Reglamento se aplicará como hasta ahora a responsables o encargados de tratamiento de datos ampliándose a los 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 nombrando un representante en la Unión Europea, que actuará como punto de contacto de las Autoridades de supervisión y de los ciudadanos y que 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.

El Reglamento introduce nuevos elementos:

El derecho al olvido. 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, implica que el interesado puede eliminar 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.

El derecho a la portabilidad. Significa 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 transferir los datos directamente al nuevo responsable designado por el interesado.

Se establece que la edad en la que los menores pueden prestar 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. Permitiendo rebajar esa edad y que cada Estado miembro establezca la suya propia, estableciendo un límite inferior de 13 años. En España, se sitúa en los 14 años. Por debajo de esa edad, es necesario el consentimiento de padres o tutores.

Responsabilidad activa. Las empresas deben adoptar medidas que aseguren que están en condiciones de cumplir con los principios, derechos y garantías que el Reglamento establece, y no sólo cuando ya se ha producido una infracción para evitar que esa infracción pueda causar daños a los interesados que pueden ser muy difíciles de compensar o reparar. Para ello, se establecen una serie 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.

Algunas de las medidas que introduce el Reglamento son una continuación o reemplazan a otras ya vigentes las medidas de seguridad o de la obligación de documentación y, la evaluación de impacto y la consulta a Autoridades de supervisión.

Otras constituyen la formalización en una norma legal de procedimientos ya de uso en las empresas o que, en todo caso, formarían parte de una adecuada organización de un tratamiento de datos, como 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.

Es importante que las organizaciones lleven a cabo un análisis de riesgo de sus procedimientos para concrete 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.

### Obtención del Consentimiento.

El consentimiento, con carácter general, ha de ser libre, informado, específico e inequívoco, requiriendo 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.

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 lo que será necesario revisar los sistemas de registro del consentimiento para que sea posible verificarlo ante una auditoría.

Aunque el Reglamento no será aplicable hasta 2018, sería 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.

Fuente: Agencia Estatal de Protección de Datos



Nos definimos como una compañía consultora independiente cuyo objetivo fundamental es suministrar servicios de consultoría en las áreas de Gestión empresarial, que representen para el cliente una solución excelente, que satisfaga sus necesidades explícitas o implícitas, tenga en cuenta las regulaciones y normas aplicables, y cumpla los objetivos de plazo y coste establecidos.

## **Madrid**

C/ Campezo 3, nave 5 28022 Madrid

Tfno.: (+34) 91 375 06 80

## **Burgos**

Centro de Empresas, 73 09007 Burgos

Tfno.: (+34) 947 041 645

## **Barcelona**

C/ Plaça Universitat 3 08007 Barcelona

Tfno.: (+34) 93 013 19 49

## **Málaga**

C/ Alejandro Dumas 17 29004 Málaga

Tfno.: (+34) 95 113 69 04

## **México**

José González Varela 15 14700 Tlalpan

Tfno.: (+52) 5513 39 96 22

[www.grupoacms.com](http://www.grupoacms.com)  
[informacion@grupoacms.com](mailto:informacion@grupoacms.com)