

NUEVO REGLAMENTO DE PROTECCIÓN DE DATOS

Después de varios años de gestación, el pasado 19 de enero se publicó en el BOE el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, que entrará en vigor a los tres meses de su publicación íntegra en el Boletín Oficial del Estado.

El presente reglamento afecta tanto a las **entidades públicas como privadas**. Por lo tanto, es completamente necesario que todas las compañías adapten su política de protección de datos a las nuevas medias que vamos a exponer a continuación.

El **objetivo** del reglamento no solo es desarrollar la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, sino todas aquellas disposiciones que afecten a la protección de nuestros datos personales; como son la Ley Orgánica 15/1999, Ley 34/2002, de 11 de julio de Servicios de la Sociedad de la Información y de comercio electrónico, la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, la Directiva Comunitaria y las disposiciones e informes jurídicos que ha venido dictando la Agencia de Protección de Datos durante los últimos ocho años.

Excluye de su **ámbito de aplicación** a las personas fallecidas (a pesar de que se habilita a sus allegados a solicitar la cancelación de los datos del fallecido); a los empresarios individuales (autónomos) y las personas de contacto de una persona jurídica, siempre y cuando se utilicen estos datos única y exclusivamente para el desarrollo de la actividad profesional como empresa o autónomo. Por tanto, en el caso de que tan solo manejemos los datos de autónomos y/o personas de contacto de una empresa, no deberemos aplicar las medias del presente reglamento.

Nos facilita un amplio elenco de **definiciones** de aquellos términos relacionados con esta materia.

En cuanto a la **obtención del consentimiento**, se regula un exhaustivo procedimiento para tratar los datos, debiendo facilitar a los afectados un plazo de 30 días y un método sencillo y gratuito manifestar su negativa a tratar sus datos. Asimismo, no podremos solicitar de nuevo el consentimiento en el plazo de un año a aquellas personas que nos lo haya denegado.

En lo que respecta a los **menores de edad**, deberemos recabar su consentimiento, utilizando un lenguaje comprensible y un método que nos permita comprobar la edad y autenticar el consentimiento paterno. No podremos recabar de los menores, datos de sus padres o tutores; y, para recabar el consentimiento de los menores de 14 años, deberemos obtener el de sus padres y tutores.

Asimismo, se establecen rigurosos **procedimientos** para los Responsables del tratamiento de datos a la hora de cumplir con los **derechos de acceso, modificación, cancelación y/o revocación del consentimiento**: se deberá dar una respuesta al afectado en el plazo de 10 días, facilitando un procedimiento sencillo y gratuito para el ejercicio de los derechos y, lo que es más importante, debiendo conservar la prueba de que hemos informado al afectado de las condiciones del tratamiento de sus datos, de la finalidad así como de la forma de ejercicio de sus derechos.

En lo que respecta a los **encargados del tratamiento**, no basta con la suscripción del contrato entre el Encargado y el Responsable del tratamiento; sino que, se deberán cumplir los siguientes requisitos: se deberá regular expresamente la posibilidad de subcontratación de los servicios y las condiciones en las que ésta se

puede dar; obligación de que el Encargado certifique que reúne las garantías para el cumplimiento de la ley en esta materia; que los empleados del Encargado conozcan y asuman el cumplimiento de las medidas de seguridad para el tratamiento de los datos; así como, que conste en el Documento de Seguridad del Encargado las medidas de seguridad que adopta en el tratamiento de los datos del Responsable.

Asimismo se establecen semejantes medidas para aquellas empresas de limpieza y mantenimiento respecto al Responsable del tratamiento.

Importantes novedades son las específicas regulaciones de los **Ficheros de publicidad y prospección comercial, videovigilancia y ficheros de solvencia y crédito**. Para poder enviar publicidad a nuestros clientes deberemos facilitarles un procedimiento sencillo y gratuito para mostrar su negativa, como es el procedimiento de la casilla en blanco. En el caso de que un afectado decida cancelar sus datos deberemos preocuparnos de cancelar los mismos incluso de los ficheros de los encargados de tratamiento, de tal forma que podamos garantizar que no volverá a recibir comunicaciones de nuestra parte. Para lo cual, podremos incluso crear un Fichero de Usuarios que no desean recibir publicidad y, en el caso de que se creen estos, tendremos la obligación de consultarlos antes de enviarles información comercial.

Se establece una prolija regulación de los **Ficheros de soporte papel**, debiendo de aplicar una serie de medidas que garanticen la correcta conservación, acceso y custodia a los documentos, respetando las medidas que se correspondan con su nivel de seguridad, ya sea básico, medio o alto.

Precisamente, en lo referente a las **medias de seguridad**, se reduce a nivel medio las medidas que se exigen para aquellos ficheros cuya única finalidad sea la gestión de nóminas.

Se imponen medidas de nivel medio a aquellos Ficheros de Entidades Gestoras, Mutuas y Servicios Comunes de la Seguridad Social y, a todos aquellos ficheros que contengan **datos que permitan deducir la personalidad** o comportamiento de una persona física, como por ejemplo los procesos de selección de personal.

De igual forma, se exigen medidas de nivel medio para aquellos Ficheros que contengan datos de tráfico y localización, cuyos responsables sean los **operadores de comunicaciones electrónicas** disponibles al público o prestadores de servicios de redes mundiales informáticas, debiendo incluso establecer un registro de acceso a los datos que permita conocer quién y cuando a intentado acceder y si finalmente ha accedido a los mismos.

A fin de poner un poco de orden en el emergente mercado de la protección de datos, se obliga a los **productos de software**, destinados al tratamiento de datos personales, que informen del nivel de seguridad que permite alcanzar ese producto.

Es un Reglamento que establece de forma prolija cómo debe estructurarse y confeccionarse el **Documento de Seguridad**, exigiendo, aún más si cabe, al confección y cumplimiento de todas las medidas de seguridad, (copias de seguridad y verificación de funcionamiento cada seis meses, exhaustivo control de acceso a la información estableciendo una política de mesas limpias, estricto conocimiento y cumplimiento de las medidas establecidas de seguridad a todo el personal que tenga o pueda tener acceso a los datos, identificación de soportes con lenguaje de códigos solo comprensible al personal autorizado.

Quedamos a su entera disposición para resolver cualquier duda que les surja al respecto.