

NOVEDADES DEL NUEVO REGLAMENTO DE MEDIDAS DE SEGURIDAD QUE DESARROLLA LA LEY 15/1999, DE PROTECCIÓN DE DATOS DE CARACTER PERSONAL

Con fecha 19 de enero del presente ha sido publicado en el BOE el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la actual Ley Orgánica de Protección de Datos Personales, Ley 15/1999. Dicha nueva regulación entrará en vigor a los tres meses de su publicación, por lo que a partir del 19 de abril del 2008, todas las empresas deberán cumplir con las nuevas medidas de seguridad que en el mismo se indican. Este Reglamento regula por primera vez las medidas a adoptar en los ficheros automatizados que en el anterior (Real Decreto 994/1999, de 11 de junio) carecían de regulación expresa.

Las innovaciones más reseñables son la aplicación de medidas de seguridad también para los ficheros no automatizados, es decir, aquellos que se encuentren en soporte papel; la regulación de un procedimiento para garantizar que cualquier persona, antes de consentir la recabación de sus datos, pueda tener un pleno conocimiento de la utilización de los mismos; la posibilidad del interesado a ejercitar el derecho de cancelación, oposición y supresión de sus datos de forma sencilla y gratuita; el incremento de medidas de seguridad en lo que se refiere a ficheros de nivel básico y medio; la consideración de los datos de minusvalía y afiliación sindical como básicos en los ficheros de nóminas; la regulación del tratamiento de datos de los menores de edad; la exigencia de nuevos requisitos para la incorporación de datos en ficheros de solvencia patrimonial y de crédito; la regulación de las actividades de publicidad y prospección comercial; la regulación de la tarjeta sanitaria; la exigencia de que los productos de software destinados al tratamiento automatizado de datos personales incluyan en su descripción técnica el nivel de seguridad que permitan alcanzar de acuerdo con lo establecido en las medidas de seguridad de este nuevo Reglamento, entre otros.

En el ámbito empresarial debemos hacer especial mención, en cuanto a los niveles de seguridad de los ficheros, a lo siguiente:

- 1.- Los ficheros de las entidades gestoras y de servicios comunes de la Seguridad Social con relación al ejercicio de sus competencias y las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social pasan de nivel básico a nivel medio.
- 2.- Desaparece el nivel básico calificado con relación a datos personales que ofrezcan una definición de las características o personalidad de los interesados y que permitan evaluar determinados aspectos de la personalidad o de su comportamiento, pasando a ser de nivel medio.
3. – A los ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas, respecto a los datos de tráfico y a los datos de localizaciones, se aplicarán además de las medidas de seguridad de nivel medio, la medida de seguridad de nivel alto de registro de accesos.

4. - Pasan a considerarse ficheros de nivel básico los que contengan datos de ideología, afiliación sindical, salud o religión cuando:
- a) Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los interesados sean asociados o miembros.
 - b) Se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad.
 - c) Los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, tengan por única finalidad cumplir una obligación legal.

Con relación a las medidas de seguridad específicas para los ficheros y tratamientos no informatizados:

1. - Se exige la aplicación de criterios de archivo que garanticen la correcta conservación de los mismos.
2. - Los armarios y archivadores deben cerrarse y mientras la información no está archivada, sobre todo aquella que hace referencia a datos especialmente protegidos, deben ser custodiados por una persona al cargo de la misma.
- 3.- Limitaciones a la realización de copias y reproducciones y a la destrucción de la documentación.
- 4.-Deberán someterse, al menos cada dos años, a una auditoria interna o externa que verifique el cumplimiento de las medidas de seguridad de Nivel Alto.

Para el cumplimiento de las nuevas medidas de seguridad se establece un régimen transitorio de implantación de las mismas:

- a) Ficheros documentales: un año desde el 19 de abril del 2008 para las medidas de seguridad de Nivel Básico; 18 meses para las de Nivel Medio y dos años para las de Nivel Alto.
- b) Ficheros automatizados: un año para los que pasan de Nivel Básico a Medio y Alto.
- c) Para todos aquellos ficheros, automatizados o no, que se creen con posterioridad en la entrada en vigor de este Reglamento no hay ningún plazo transitorio de adaptación, debiendo tener implantadas las medidas de seguridad desde el omento de la creación de los ficheros.

Con respecto a los ficheros sobre solvencia patrimonial y crédito se exige la existencia previa de una deuda cierta, líquida y exigible que haya resultado impagada y que no se haya iniciado una reclamación arbitral, judicial o administrativa de la misma antes de incluir esos datos en un fichero. Se obliga al mismo tiempo a comunicar previamente al deudor la inclusión en el fichero y se establece la responsabilidad del acreedor en caso de que aporte datos inexactos, así como se prohíbe también mantener los ficheros con el dato "saldo cero".

En cuanto a las actividades de publicidad y prospección comercial, es necesario que la entidad que contrate con una empresa la realización de una campaña publicitaria se asegure que ésta ha recogido los datos cumpliendo con todo lo establecido en la Ley. Será asimismo obligatorio el consentimiento del interesado a fin de que los responsables de los diferentes ficheros puedan cruzar sus datos para promocionar y comercializar productos y servicios. Se regulan también las denominadas "listas Robinson" o listas de exclusión mediante las cuales el interesado puede comunicar al responsable de un fichero que no quiere recibir publicidad y esas listas serán de obligada consulta previa para todos aquellos que realicen tareas de publicidad y prospección comercial.

Respecto a la externalización de servicios, el Encargado del tratamiento contratado podrá subcontratar algunos de los servicios, pero tendrá que estar previamente autorizado por el Responsable del Fichero. Se prevé también que cuando el responsable del fichero contrate la prestación de un servicio que comporte un tratamiento de datos por terceros deberá velar para que el encargado del tratamiento reúna las garantías para el cumplimiento de lo dispuesto en el Reglamento, en especial todo aquello que se refiere a la conservación y seguridad de los datos personales.

En cuanto al régimen de las auditorias de seguridad, a partir del nivel medio, los sistemas de información e instalaciones de tratamiento y almacenamiento de datos deberán someterse, al menos cada dos años, a una auditoria interna o externa que verifique el cumplimiento de las medidas de seguridad correspondientes, ahora también para los ficheros en soporte documental.

Sobre la potestad sancionadora de la Agencia Española de Protección de Datos, debemos indicar que no se han modificado las infracciones, sanciones ni cuantía de las multas, pero sí que se ha introducido un límite temporal de 12 meses a la duración de la incoación de un expediente sancionador, y que una vez transcurrido dicho plazo sin que se hubiera notificado acuerdo de inicio de un procedimiento sancionador, todas las actuaciones previas se entenderán caducadas.