ADECUACION PROTECCION DE DATOS PERSONALES. REGLAMENTO EUROPEO

La obligación del cumplimiento de la normativa sobre protección de datos de carácter personal está especialmente ligada con la actividad diaria de las empresas, puesto que éstos son un activo importante para el quehacer de las mismas. El tratamiento de datos personales está ocasionando importantes riesgos económicos asociados al, de por sí, incumplimiento de la normativa vigente en dicha materia. El desarrollo de la actividad de la mayoría de las empresas obliga al establecimiento y adopción de una serie de medidas legales, técnicas y organizativas de seguridad que limiten su responsabilidad frente a posibles incumplimientos de la normativa. Esta adaptación ha de realizarse de una forma exhaustiva y personal acorde a los diferentes ámbitos de actuación y desarrollo empresarial, puesto que entendemos que cada empresa es diferente, inclusive dentro del mismo sector de actividad.

La protección de datos personales se encuentra regulada en la **Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal -**en adelante, **LOPD-** y en el **Real Decreto 1720/2007** en el cual se desarrolla dicha ley orgánica -en adelante, **RDLOPD**-, ambas de obligado cumplimiento para las empresas y autónomos, indistintamente de su tamaño, organización o ámbito de actividad. El objetivo de la mencionada normativa es la protección que de los datos personales realiza la empresa, entendiéndose por dato personal cualquier información concerniente a personas físicas identificadas o identificables, es decir, aplicable a la información que la empresa pueda disponer de sus trabajadores, proveedores, clientes, consumidores, etc. Además, dicha normativa regula el tratamiento de esos datos, es decir, todas aquellas operaciones y procedimientos técnicos, de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

Con la entrada en vigor del Reglamento Europeo de Protección de Datos Personales el pasado 25 de mayo del 2016, se abre un nuevo escenario regulatorio, puesto que dicho Reglamento es de aplicación directa a España y, por tanto, prevalecerá sobre cualquier normativa estatal vigente, es decir, primará su aplicación respecto a la actual **LOPD** y **RDLOPD**. Este nuevo escenario, que entrará en vigor en mayo de 2018, incorpora importantes novedades que hacen preciso iniciar los procesos de adecuación, tal y como recomienda la propia Agencia Española de Protección de Datos.

"[…] puede ser 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 […] En general, las organizaciones que tratan datos personales deberían comenzar a preparar la aplicación de estas medidas, así como de otras modificaciones prácticas derivadas del Reglamento […]

Entre las principales novedades que incorpora el nuevo reglamento europeo, destacan los siguientes extremos:

En el ámbito organizativo:

- Designación de la figura denominada DPO o Delegado de Protección de Datos Personales, cuya principal misión es velar por el cumplimiento normativo dentro de la entidad respecto al tratamiento de datos personales.
- La comunicación de brechas de seguridad que pudiere acontecer dentro de la actividad diaria de la entidad.

- La eliminación de registrar ficheros, sustituyendo dicha obligación por la llevanza de un control interno de la información personal tratada.

En el ámbito técnico:

- La principal novedad es la sustitución del denominado Documento de Seguridad por Protocolos o Programas de tratamiento de datos personales, en el cual se hará constar todos aquellos protocolos que se encuentren implementados en la empresa en materia de seguridad de la información, insertando organigrama de las nuevas implicaciones en materia de adecuación al GDPR.
- La necesidad de efectuar Evaluaciones de Impacto o Evaluaciones de Riesgo y documentar aquellas antes de efectuar cualquier operación automatizada respecto a un tratamiento masivo de datos.

En el ámbito legal:

- La modificación de la forma de obtener el consentimiento para el tratamiento de datos personales de los afectados o, actualmente, denominados interesados. Dicho consentimiento deberá ser explícito, es decir, expreso siempre.
- La incorporación de gifs o imágenes que permitan a los usuarios acceder de una forma sencilla a la forma de tratar los datos.
- La incorporación y realización de una política de transparencia respecto al organigrama técnico y legal de la información personal a tratar.

En el ámbito sancionador:

- Sanciones administrativas cuyo importe pudiere alcanzar los 20 MILLONES DE EUROS o el 4% del volumen de negocio total anual.
- La posibilidad que el interesado o afectado pueda exigir a la entidad daños y perjuicios por el tratamiento efectuado.
- La inclusión de sanciones penales por el tratamiento indebido de datos de carácter personal.

Esta situación supone que las entidades no solo deben cumplir con la actual normativa estatal vigente en materia de protección de datos personales sino que, adicionalmente, deben efectuar las actualizaciones correspondientes para que en mayo de 2018 estén completamente ajustadas al nuevo marco europeo de protección de datos personales.

Fases de Control y Garantías del GDPR. Tipos de Auditoría