El nuevo Reglamento 1720/2007 sobre Protección de Datos. Crónica de un nuevo reglamento anunciado.

El pasado día 19 de Abril entró en vigor el Real Decreto 1720/2007 sobre Protección de Datos de Carácter Personal, el cuál fue publicado el 9 de Enero en el BOE núm. 17 de 2008. Desde su entrada en vigor, se establece un plazo de un año para implantar las medidas de seguridad derivadas, lo que nos obliga a adaptarnos al nuevo Reglamento en el desarrollo de nuestra actividad, pero… ¿conocemos en qué medida nos afecta esta adaptación?, ¿hemos llegado a cumplir los requisitos establecidos por el derogado ya derogado Reglamento 1332/1994 ó por el RD 994/1999 para poder hablar de adaptación?

Estructura y objeto del nuevo Reglamento

Parafraseando a Gabriel García Márquez, con su novela corta publicada en 1981, tan sólo pretendemos captar la atención del lector para anunciarle que nos encontramos ante un nuevo Reglamento que, en realidad, no es tan nuevo, pero sin embargo, nos presenta toda una serie de novedades que debemos conocer si queremos asegurar el cumplimiento de los requisitos que establece con total seguridad. Y digo no es tan nuevo, porque este Real Decreto no es más que la actualización de un Real Decreto, el RD 994/1999, que se correspondía con la antigua LORTAD. Y si ésta se actualizó el 13 de Diciembre de 1999 en la conocida LOPD, podemos considerar que el nuevo Reglamento de Medidas de Seguridad era una asignatura pendiente en tanto en cuanto nos encontrábamos ante un vacío normativa en relación con el tratamiento a dar a ficheros de datos personales no automatizados.

Varios son los aspectos tratados por el nuevo Reglamento. Con una estructura basada en nueve títulos, este Reglamento comparte con la LOPD el fin garantizar la integridad, la seguridad y la confidencialidad en el tratamiento de datos personales y nace con vocación de desarrollar los contenidos de la norma superior pero ante todo, de clarificar aquellos aspectos que en estos años, se ha puesto en evidencia que precisan de mayor desarrollo normativo.

Los títulos incluidos en esta Norma son:

- Título I: Objeto y Ámbito de Aplicación. Cabe destacar la aclaración de qué se entiende por ficheros y tratamientos relacionados con actividades personales o domésticas, ya que ésos se excluyen del ámbito de ésta normativa, así como inclusión de una serie de definiciones que ayudan al correcto entendimiento de la Norma.

- Título II: Principios de protección de Datos. Especial atención a la regulación del modo de captación del consentimiento atendiendo a aspectos muy específicos como el caso de servicios de comunicaciones electrónicas y, muy especialmente, a la captación de datos de menores.

- Título III: Derechos de las personas en materia de protección de datos. Acceso, rectificación, cancelación y oposición al tratamiento a partir de la efectiva imposición a terceros de los mencionados deberes de hacer.

- Título IV a VII: Clarifican aspectos básicos para el tráfico ordinario, el deber de los responsables de creación e inscripción de los ficheros, , los criterios y procedimientos para la realización de las transferencias internacionales de datos y la regulación del código tipo como instrumento dinamizador del derecho fundamental a la protección de datos.

- Título VIII: Regula la seguridad en el tratamiento de datos personales.

- Título IX: Dedicado a los procedimientos tramitados por la Agencia Española de Protección de Datos (APD).

El presente reglamento deroga a los siguientes documentos:

- Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la ley orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.

- Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal

- Todas las normas de igual o inferior rango que contradigan o se opongan a los dispuesto en el nuevo real Decreto.

Este Reglamento nace con vocación de desarrollar los contenidos de la norma superior pero ante todo, de clarificar aquellos aspectos que en estos años, se ha puesto en evidencia que precisan de mayor desarrollo normativo.

Consideraciones e interpretaciones

Desarrollado ya el objeto y la estructura del documento, no podemos hacer otra cosa que adentrarnos en su contenido y perdernos entre sus líneas durante un total de 35 páginas estructuradas en dos columnas, para poder afirmar que dos son los ejes principales en torno a los cuales se desarrolla en Reglamento. En primer lugar, llama la atención el tono aclaratorio de un documento que viene a aclarar muchos conceptos que hasta la fecha han sido difícilmente interpretables y dada la especial sensibilidad del objeto de tratamiento, era básica una aclaración que, por si bien por la mayoría es bien recibida, son muchos los que han manifestado sus críticas al respecto. En segundo lugar, la definición de medidas de seguridad específicas para el tratamiento de ficheros no automatizados así como la ampliación de medidas relacionadas con la gestión de soportes y su destrucción.

Vale la pena desarrollar el artículo 2, *Ámbito objetivo de aplicación*, que en su apartado segundo, textualmente dice: *"Este Reglamento no será aplicable a los tratamientos de datos referidos a personas jurídicas, ni a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados. Así como la dirección postal o electrónica, teléfono y número de fax profesionales".* Pues bien… ¿a qué nos conduce esta aclaración? Nos conduce a aclarar por fin, qué debemos hacer con los contactos profesionales que tenemos después de asistir a una feria, o de intercambiar tarjetas en una reunión de trabajo con clientes o proveedores. Nos conduce a saber cómo tratar los datos de autónomos o profesionales independientes. Nos conduce a reducir el número de ficheros a inscribir en la Agencia y sobre todo, nos conduce a simplificar los trámites administrativos a cumplir para poder hacer uso de un contacto de qué podamos disponer a nivel profesional. Porque si bien, el no ser objeto de aplicación el tratamiento de datos de personas de contacto de empresas clientes o proveedores

no exime de la necesidad de tratar este tipo de datos con integridad y confidencialidad, es cierto que el conjunto de medidas de seguridad tanto a nivel técnico como organizativo a aplicar y los requisitos administrativos a cumplir, son aspectos que en muchas ocasiones, ahogan a las empresas que forman la mayoría del tejido empresarial que nutre nuestra economía y debemos aplaudir toda iniciativa que acerque la responsabilidad empresarial con la realidad actual.

Y… si la identificación de este conjunto de datos como excluidos del ámbito de aplicación resulta claramente definida, no ocurre lo mismo en relación con los datos de los trabajadores de la empresa que está aplicando las medidas establecidas por el RDLOPD, siendo prueba de ello la polémica existente en la interpretación de este apartado al efecto. Por un lado, podemos considerar que los datos de los trabajadores de una Organización se limitan a datos profesionales, pero… ¿qué hacemos con los datos del Curriculum Vitae? Porque, si no disponemos de un formato acotado al contenido a cumplir por parte del personal, es muy común encontrar datos como hobbies, estado civil e incluso, a estas alturas, situación militar! Además, ¿Cuántos trabajadores están afiliados a sindicatos y se les descuenta la cuota sindical de la propia nómina?, ¿No conocemos el estado de salud de nuestros compañeros de trabajo?... en fin, como podemos comprobar, el entramado y la cantidad de información de que puede disponer una empresa de sus trabajadores aconsejan que se traten con especial cautela todos los datos personales disponibles ya que al fin y al cabo, el fin último de la normativa es la preservación de los derechos de los titulares sobre sus propios datos.

4 Elementos básicos en la adaptación al nuevo Reglamento

1 PLAZOS

En primer lugar, debemos conocer los plazos establecidos para la adaptación al nuevo Reglamento establecidas en líneas generales, por el mismo:

- Ficheros automatizados existentes en la fecha de entrada en vigor del nuevo Real Decreto:
  - 12 meses para la aplicación de medidas de seguridad básico y medio con carácter general.
  - 18 meses para la aplicación de medidas de seguridad de nivel alto, para ficheros que contengan datos relacionados con:
    - Violencia de género
    - Operadores de servicios de comunicaciones electrónicas disponibles al público o que exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico o localización.

- Ficheros no automatizados que existieran en la fecha de entrada en vigor del nuevo Real Decreto:

- 12 meses para la aplicación de medidas de seguridad de nivel básico
- 18 meses para la aplicación de medidas de seguridad de nivel medio
- 18 meses para la aplicación de medidas de seguridad de nivel alto

- Ficheros creados con posterioridad a la entrada del nuevo Real Decreto:
  - La totalidad de medidas de seguridad deberán ser aplicadas desde el momento de su creación.

2 ADAPTACIÓN DEL DOCUMENTO DE SEGURIDAD

Una vez identificados los ficheros sujetos al ámbito de aplicación del Reglamento, debemos actualizar el Documento de Seguridad, el cual, debe erigirse como epicentro de nuestro sistema de gestión para la protección de datos de carácter personal y no como una guía o transcripción de la colección de artículos definidos en la normativa de referencia. Debemos aprovechar el Documento de Seguridad como herramienta en la que reflejar todas y cada una de las medidas a aplicar y para clarificar cualquier aspecto relacionado con los ficheros de que disponemos y las funciones y responsabilidades asociadas.

El contenido principal del Documento de Seguridad debe comprender:

1. Ámbito de aplicación del documento.
2. Medidas, normas, procedimiento, reglas y estándares encaminados a garantizar los niveles de seguridad exigidos en este documento.
3. Procedimiento general de información al personal.
4. Funciones y obligaciones del personal.
5. Procedimiento de notificación, gestión y respuestas ante incidencias.
6. Procedimientos de revisión.
7. Consecuencias del incumplimiento del Documento de Seguridad.

Otros contenidos a contemplar, son:

1. Aspectos específicos relativos a los diferentes ficheros
2. Nombramientos
3. Autorizaciones firmadas para la salida o recuperación de datos
4. Inventario de soportes
5. Registro de incidencias
6. Contratos o cláusulas aplicables a encargados del tratamiento
7. Registro de entrada y salida de soportes

3 NIVELES DE SEGURIDAD

Se mantiene la clasificación de los ficheros en tres niveles acumulativos: básico, medio y alto en función de la naturaleza de la información tratada.

Nivel Alto:

- Ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual, los recabados con fines policiales sin consentimiento del afectado y los derivados de violencia de género.

Nivel Medio:

- Datos relativos a la comisión de infracciones administrativas o penales
- Datos derivados de la prestación de servicios de solvencia patrimonial y crédito
- Ficheros de datos de Administraciones Tributarias
- Ficheros de datos de Entidades Financieras
- Ficheros de datos de Entidades Gestoras y Servicios Comunes de Seguridad Social
- Ficheros de datos e mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social
- Ficheros de datos que ofrezcan una definición de la personalidad y permitan evaluar determinados aspectos de la personalidad o el comportamiento de las personas
- Ficheros de datos de los operadores de comunicaciones electrónicas en relación con datos de tráfico y localización.

Nivel Básico:

Se aplicarán a cualquier otro fichero que contenga datos de carácter personal incluyendo a aquellos ficheros que contengan datos de ideología, afiliación sindical, religión, creencias, salud, origen racial o vida sexual cuando:

- Los datos se usen por parte de asociaciones con fines de realizar transferencias dinerarias por parte de sus asociados o miembros.
- Se trate de datos en soporte no automatizado cuando se dispongan de forma accesoria o complementaria que no guarden relación con la finalidad del fichero
- Ficheros que contengan datos de salud cuando se refieran exclusivamente al grado o condición de discapacidad o declaración de invalidez con motivo del cumplimiento de deberes públicos.

4 MEDIDAS DE SEGURIDAD

A continuación, presentamos un cuadro resumen de medidas de seguridad que podemos encontrar en la página web de la propia Agencia española de Protección de Datos (www.agpd.es).

	N. BÁSICO		
	N. MEDIO		
	N. ALTO		
RESPONABLE DE SEGURIDAD		Designar	
PERSONAL	- Funciones definidas - Difusión de Normas		
INCIDENCIAS	- Registro de Incidencias - Procedimiento de notificación y gestión	SOLO FICHEROS AUTOMATIZADOS - Disponer de Procedimientos - Autorización del responsable para recuperar datos	
CONTROL DE ACCESO	- Relación de usuarios y accesos autorizados - Control de accesos permitidos - Concesión de permisos	SOLO FICHEROS AUTOMATIZADOS - Control de acceso físico a locales	MEDIDAS ESPECIFICAS PARA FICHEROS AUTOMATIZADOS Y MEDIDAS ESPECIFICAS PARA FICHEROS NO AUTOMATIZADOS
IDENTIFICACIÓN Y AUTENTICACIÓN	SOLO FICHEROS AUTOMATIZADOS - Identificación personalizada - Procedimiento de gestión de contraseñas - Almacenamiento ininteligible de contraseñas	SOLO FICHEROS AUTOMATIZADOS - Límite de intentos de acceso no autorizados	
GESTIÓN DE SOPORTES	- Inventario de soportes - Identificación de contenidos - Accesos limitados	SOLO FICHEROS AUTOMATIZADOS - Registro de Entrada y Salida de soportes	SOLO FICHEROS AUTOMATIZADOS - Etiquetado confidencial - Cifrado en distribución - Cifrado en dispositivos portátiles
COPIAS DE RESPALDO	SOLO FICHEROS AUTOMATIZADOS - Copia semanal - Procedimientos de generación y custodia - Verificación semestral - Pruebas con datos reales		SOLO FICHEROS AUTOMATIZADOS - Ubicación de copia y sistema diferentes

CRITERIOS DE ARCHIVO	SOLO FICHEROS NO AUTOMATIZADOS - Criterios de archivo		
ALMACENAMIENTO	SOLO FICHEROS NO AUTOMATIZADOS - Dispositivos de almacenamiento con mecanismos que dificulten su apertura		SOLO FICHEROS NO AUTOMATIZADOS - Áreas y equipamientos protegidos con llave
CUSTODIA DE SOPORTES	SOLO FICHEROS NO AUTOMATIZADOS - Custodia responsable		
COPIA O REPRODUCCION			SOLO FICHEROS NO AUTOMATIZADOS - Sólo realizable por personas autorizadas - Destrucción de copias desechadas
AUDITORIA		- Cada dos años - Interna o externa - Informe con deficiencias y acciones correctoras propuestas - Análisis del responsable y conclusiones	
TELECOMUNICACIONES			SOLO FICHEROS AUTOMATIZADOS - Transmisión electrónica cifrada
TRASLADO DOCUMENTACIÓN			SOLO FICHEROS AUTOMATIZADOS - Impedir acceso o manipulación mediante medidas

- Fuente: Guía de Seguridad publicada por la AEPD y disponible en www.agpd.es

Conclusiones

Realizadas ya las debidas presentaciones, realizadas ya las consideraciones e interpretaciones más destacables, bajo mi humilde punto de vista, y realizados ya los desarrollos de aquellos aspectos fundamentales a considerar para poder entrar de lleno en la sinuosa aventura de adaptarnos al nuevo RDLOPD, tenemos todos los ingredientes necesarios para poder afrontar este reto. Al fin y al cabo, una lectura detenida de la normativa existente en la materia, debe ser suficiente para comprender el alcance de todos y cada uno de los requisitos que establece o por lo menos, de sensibilizarnos ante el fin que persigue. La AEPD destacaba en una publicación del 2 de Abril de 2008 que más de un 70% de los ciudadanos se muestra preocupado por la Protección de Datos a tenor de los datos publicados en el Barómetro del CIS de Febrero de 2008, Estudio nº 2.758. Ante esta tendencia… ¿no vale la pena realizar un esfuerzo y asegurar así la integridad, la seguridad y la confidencialidad de los datos que tratamos diariamente? Seguro que sí.

Guillermo Campamá
Socio Consultor y Auditor de Empresas
EuQuality Networks, S.L.

gcampama@euquality.net
902.196.851