

Novedades del Reglamento de Protección de Datos

Jornada TIC, 13 marzo 2008

SATipyme Zaragoza

Javier Prenafeta Rodríguez
Abogado

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

Deroga:

- 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
- Real Decreto 1332/1994, de 20 de junio, que desarrolla determinados aspectos de la Ley Orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal

Principales novedades:

- Describe y amplía las previsiones de la ley en cuanto a **principios, ejercicio de los derechos**, ficheros sobre solvencia patrimonial y crédito y publicidad y prospección comercial, creación y notificación de ficheros, transferencias internacionales de datos, códigos tipo y diversos procedimientos ante la AGPD.
- Amplía las **medidas de seguridad** a los **ficheros no automatizados** (papel) y reforma las establecidas en general para ficheros automatizados.

Ámbito de aplicación: ficheros excluidos

1. Ficheros de personas jurídicas
2. Ficheros de personas físicas para actividades personales o domésticas
3. Protección de materias clasificadas, investigación del terrorismo y otras formas de delincuencia organizada
4. Ficheros de personas físicas que presten servicios en personas jurídicas (agenda de contactos, tarjeteros,...)
5. Ficheros de empresarios individuales: comerciantes, industriales o navieros, siempre que la finalidad del tratamiento se relacione con dichas actividades comerciales o mercantiles
6. Ficheros de personas fallecidas

Ficheros de Administraciones Públicas

Régimen doble:

- Público: AAPP en el ejercicio de competencias y funciones públicas
- Privado: corporaciones de derecho público para actividades fuera del régimen de las AAPP

Especialidades en el consentimiento para el tratamiento de datos y cesiones

Datos de menores de edad

Forma: expresa o tácitamente (30 días)

Comunicación en informaciones o facturación periódica

Mecanismos gratuitos para manifestar la oposición o revocación del consentimiento

Reestructuración de sociedades

Tratamiento de datos por cuenta de tercero

Acceso y uso de datos en interés de tercero en el marco de una relación comercial preexistente

Responsabilidad en casos de extralimitación: titular del fichero

Se admite subcontratación:

- Autorización o previsión en el contrato
- Se determine o cumunique la entidad subcontratada

Ejercicio de los derechos de acceso, oposición, rectificación y cancelación

Representación voluntaria, además de incapacitados o menores de edad

Medio sencillo y gratuito

Procedimiento:

- Nombre y domicilio, fotocopia DNI o equivalente, autorización en representación, fecha y firma
- Resolución en el plazo de un mes, en derecho de acceso, debiendo hacerse efectivo dentro de los 10 días siguientes
- Resolución en el plazo de 10 días, en derechos de rectificación, oposición y cancelación

Ficheros de solvencia patrimonial y crédito

Ejercicio de los derechos no está sujeto a restricciones de tiempo (12 meses), normativas o supeditadas a la relación negocial existente entre las partes

Requisitos de incorporación:

- Deuda cierta, vencida, exigible e impagada
- Requerimiento previo de pago
- Inexistencia de un principio de prueba que contradiga lo anterior

Notificación al afectado dentro de los 30 días siguientes al registro (una por deuda)

Cancelación:

- Inmediatamente, efectuado el pago o cumplimiento de la deuda
- A los 6 años desde el vencimiento de la obligación, en todo caso

Ficheros para actividades de publicidad o prospección comercial

Deber de información en cada comunicación que se dirija, en caso de fuentes accesibles al público.

Campañas publicitarias: responsabilidad de los ficheros en función de quien determine los parámetros de identificación de los destinatarios.

Ficheros de exclusión, generales o sectoriales. Listas Robinson

Transferencias internacionales de datos

Salida de datos fuera del Espacio Económico Europeo

Autorización del Director de la AGPD, salvo excepciones:

- Nivel de protección equiparable al estándar europeo,
- Consentimiento inequívoco a la transferencia concreta,
- En virtud de tratados o convenios internacionales en los que España sea parte, auxilio judicial internacional, asistencia y diagnóstico médicos, transferencias dinerarias, ejecución de un contrato...

Códigos tipo

Contenido y modelos:

- Cláusulas tipo para la obtención del consentimiento,
- Cláusulas tipo para informar a los afectados del tratamiento,
- Modelos para el ejercicio por los afectados de sus derechos de acceso, rectificación, cancelación y oposición,
- Modelos de cláusulas para el cumplimiento de los requisitos formales exigibles para la contratación de un encargado del tratamiento, en su caso

Depósito y registro en la AGPD

Evaluación periódica y memoria de actividades anual

MEDIDAS DE SEGURIDAD

Modificaciones en la determinación de los niveles:

- Nivel medio:
 - Datos de localización y tráfico de operadores de telecomunicaciones + registro de accesos para nivel alto
 - Ficheros de entidades financieras para prestación de estos servicios
 - Ficheros de Entidades Gestoras y Servicios Comunes de la Seguridad Social, mutuas de accidentes de trabajo y enfermedades profesionales
- Nivel alto: actos relacionados con la violencia de género
- Nivel básico: datos especialmente protegidos
 - Transmisiones dinerarias
 - Tratamiento incidental o accesorio en ficheros no automatizados
 - Tratamiento del grado de discapacidad o su simple condición en cumplimiento de deberes públicos.

Medidas para tratamientos automatizados

Nivel básico:

- Documento de Seguridad, que deberá hacer referencia a los encargados de tratamiento, en su caso, y al contrato con éstos.
- Determinación de funciones y obligaciones del personal.
- Registro de incidencias: tipo, fecha/hora, personas implicadas, efectos y medidas correctoras.
- Control de acceso a los datos con sistema de identificación y autenticación inequívoca y personalizada para cada usuario. Gestión de contraseñas, con duración no superior a un año.
- Inventario e identificación de soportes.
- Autorización del Responsable del fichero o bien de antemano en el Documento de Seguridad para salida de soportes y documentos fuera de los locales o instalaciones (también correos electrónicos).
- Realización de copias de seguridad (semanalmente) y sistema de restauración (comprobación cada 6 meses).

Nivel medio:

- Responsable de Seguridad
- Auditoría bienal
- Sistema de gestión de entradas y salidas de soportes y documentos: tipo de documento o soporte, fecha/hora, emisor o destinatario, número de documentos o soportes, tipo de información que contienen, forma de envío.
- Control de acceso a los datos, impidiendo intentos reiterados de acceso. También control de acceso físico a los servidores donde se encuentran los datos.
- Constancia de las recuperaciones de datos en el Registro de Incidencias.

Nivel alto:

- Gestión y distribución de soportes de modo que se impida su identificación a personal no autorizado. Cifrado de los datos.
- Almacenamiento de una copia de seguridad y los procedimientos de recuperación fuera de los locales de tratamiento.
- Control de accesos: identificación de usuario, fecha/hora, fichero accedido, tipo de acceso, autorización/denegación. Conservación durante dos años. Excepción para personas físicas y usuario único.
- Cifrado de datos por redes de comunicaciones públicas (no red de área local)

Medidas para tratamientos no automatizados (papel)

Nivel básico:

- Funciones y obligaciones del personal, registro de incidencias, control de acceso, gestión de soportes.
- Definición y aplicación de un criterio lógico de archivo de los soportes o documentos.
- Utilización de soportes de almacenamiento que eviten su apertura por parte de personas no autorizadas. Excepción.
- Establecimiento de normas para la custodia de los soportes

Nivel medio:

- Responsable de Seguridad
- Auditoría bienal

Medidas para tratamientos no automatizados (papel)

Nivel alto:

- Acceso restringido a elementos de almacenaje de documentos o soportes y (las copias de seguridad de éstos): llave u otro dispositivo equivalente.
- Supervisión en la reproducción de documentos.
- Medidas que permitan identificar y registrar accesos realizados cuando los documentos se puedan utilizar por varios usuarios.
- Medidas que impidan el acceso o manipulación por terceros cuando se trasladen soportes o documentos con datos.

Plazos de implantación

A) Ficheros creados tras el 9 de abril de 2008: inmediatamente

B) Ficheros automatizados preexistentes:

Hasta el 9 de abril de 2009, medidas de nivel medio para:

- EG y SC Seguridad Social
- Mutuas de accidentes de trabajo y enfermedades profesionales
- Ficheros de perfiles o evaluación de la personalidad
- Ficheros de actos de violencia doméstica
- Ficheros de datos de tráfico y localización de operadoras de telecomunicaciones

Hasta el 9 de octubre de 2009, medidas de nivel medio para los dos últimos

Hasta el 9 de abril de 2009: resto de medidas no previstas en el Reglamento anterior

Plazos de implantación

C) Ficheros no automatizados preexistentes

Hasta el 9 de abril de 2009: nivel básico

Hasta el 9 de octubre de 2009: nivel medio

Hasta el 9 de abril de 2010: nivel alto

Cámara
Zaragoza

Gracias por su atención

SATipyme 

