



## PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

El 19 de enero de 2008 se publicó en el Boletín Oficial del Estado, el **Real Decreto 1.720/2.007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1.999, de 13 de diciembre de protección de datos de carácter personal.**

### Antecedentes Legislativos:

El presente Real Decreto no sólo nace con la vocación de no reiterar los contenidos de la norma superior **-la Ley Orgánica 15/1.999, de 13 de diciembre que transpone a nuestro ordenamiento jurídico la Directiva 95/46/CE, del Parlamento y del Consejo, de 24 de octubre-** sino de desarrollar, igualmente, aquellos que en estos años de vigencia de la Ley se ha demostrado que precisan de un mayor tratamiento legislativo.

La norma abarca la tutela de los precedentes **Reales Decretos 1.332/1.994, de 20 de junio y 994/1.999, de 11 de junio, los cuales deroga.**

Asimismo desarrolla procedimientos para el ejercicio de la potestad sancionadora de la Agencia Española de Protección de Datos **-Ley 34/2.002, de 11 de julio de Servicios de la sociedad de la información y de comercio electrónico complementada por la Ley 34/2.003, de 3 de noviembre General de Telecomunicaciones-**.

### Estructura del Real Decreto 1720/2007 de 21 de Diciembre:

El **Real Decreto 1.720/2.007, de 21 de Diciembre**, consta de **un artículo único** por el que se aprueba el reglamento, **cinco disposiciones transitorias** que regulan:

- **La adaptación de los códigos tipo inscritos en el registro general de protección de datos:** *un año desde la entrada en vigor del real decreto, como plazo en el que debe notificarse a la Agencia Española de Protección de Datos las modificaciones que resulten necesarias en los códigos de tipo inscritos en el registro general de protección de datos.*
- **Los plazos de implantación de las medidas de seguridad:** *la norma distingue entre los ficheros –tanto automatizados como no- existentes a la entrada en vigor del real decreto; respecto a los no automatizados las*

*medidas de seguridad deberán implantarse, si son de nivel básico, en el plazo de un año desde la entrada en vigor; las medidas de seguridad de nivel medio, en el plazo de dieciocho meses; y las medidas de nivel alto, en el plazo de dos años desde la entrada en vigor.*

*Para el supuesto de ficheros creados con posterioridad a la fecha de entrada en vigor del presente real decreto deberán tener implantadas en el momento de su creación la totalidad de las medidas de de seguridad reguladas en el mismo.*

- **El régimen transitorio de las solicitudes para el ejercicio de los derechos de las personas** -derechos de acceso, oposición, rectificación y cancelación- las solicitudes efectuadas antes de la entrada en vigor del real decreto, no les será de aplicación el mismo y se regirán por la normativa anterior.
- **El régimen transitorio de los procedimientos.** Lo mismo, los iniciados antes de la entrada en vigor de la norma no les será de aplicación la misma.
- Lo mismo es predicable respecto de las **actuaciones previas.**

Asimismo el instrumento de aprobación del Real Decreto consta de una disposición derogatoria por la que se derogan entre otros el Real Decreto 994/1999 de 11 de junio y dos finales, siendo de destacar que entrará en vigor *“a los tres meses de su íntegra publicación en el Boletín Oficial del Estado”*, es decir, el día 19 de abril de 2008.

Respecto al reglamento de desarrollo de la **Ley Orgánica 15/1.999, de 13 de diciembre**, de protección de datos de carácter personal propiamente dicho, éste se estructura en nueve títulos, una disposición adicional *-relativa a los productos de software destinados al tratamiento automatizado-* y una disposición final *-la aplicación supletoria del Real Decreto 1.389/1.993, de 4 de Agosto para lo no regulado en el capítulo III del Título IX del presente Real Decreto, relativo a procedimientos sancionadores-*.

**El Título I** contempla el objeto y ámbito de aplicación del reglamento *“...tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal.”*

Este Reglamento y tal y como lo contempla el art. 2, será de aplicación a los datos de carácter personal susceptibles de tratamiento. Por el contrario, **no será de aplicación**:

- 1) a los datos sobre personas jurídicas, ni a los ficheros que incorporan datos de personas físicas que prestan servicios en las personas jurídicas, y que consisten en su nombre, apellidos, funciones o puestos desempeñados, dirección postal o electrónica, teléfono y fax profesionales; y
- 2) a los datos sobre empresarios individuales, en su calidad de comerciantes, industriales o navieros.

El tratamiento de datos de carácter personal “no será susceptible de protección” en el caso de que esos datos se encuentren en “fuentes accesibles al público”, y que además de otras son:

- 1) las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección profesional e indicación de su pertenencia al grupo. La dirección profesional podrá incluir los datos del domicilio postal completo, número telefónico, número de fax y dirección electrónica. En el caso de Colegios profesionales, podrán indicarse como datos de pertenencia al grupo los de número de colegiado, fecha de incorporación y situación de ejercicio profesional.
- 2) los diarios y boletines oficiales; y
- 3) los medios de comunicación social. (art. 7)

**El Título II**, se refiere a los principios de la protección de datos, entre ellos reviste particular importancia la regulación del modo de captación del consentimiento atendiendo a aspectos muy específicos como el caso de los servicios de comunicación electrónica y, muy particularmente, la captación de datos de los menores. Aparece la figura del *-encargado del tratamiento (capítulo III)-*.

Con respecto al “**consentimiento**”, éste deberá ser recabado por el responsable del tratamiento para el tratamiento de sus datos de carácter personal, salvo en los casos en los que no sea exigible de acuerdo a la ley. El responsable deberá demostrar la existencia de este consentimiento por cualquier medio de prueba admisible en derecho. El afectado deberá ser informado de forma inequívoca sobre la finalidad a la que se destinarán los datos, así como en el caso de la cesión de los mismos se informará sobre el tipo de actividad desarrollada por el cesionario.

Una vez solicitado el consentimiento, el afectado tendrá 30 días para manifestar su negativa al tratamiento, si bien se le advertirá que en el caso de no existir pronunciamiento en este sentido se entenderá que consiente en el tratamiento de los datos de carácter personal.

Con respecto a la figura del “**encargado del tratamiento**”, y cuando exista una persona encargada del tratamiento de datos por orden del responsable del tratamiento, no se considerará que hay “comunicación” de datos, en cuyo caso existiría un nuevo vínculo entre este encargado y el afectado. En general, el encargado del tratamiento no podrá de “*motu proprio*” subcontratar el servicio del tratamiento de datos encomendado por el responsable de tratamiento, salvo que tenga autorización expresa de él, y siempre que se haga en nombre y por cuenta del responsable del tratamiento.

Cuando el responsable del fichero o tratamiento facilite el acceso a los datos a un encargado de tratamiento que se halle en los locales del responsable, deberá hacerse constar esta circunstancia en el documento de seguridad del responsable del fichero, comprometiéndose el personal del encargado de tl tratamiento a cumplir con las medidas de seguridad previstas en ese documento.

En el caso de que el servicio prestado por el encargado del tratamiento fuera en locales ajenos a los del responsable del fichero, el encargado deberá elaborar un documento de seguridad en los términos exigidos por el Reglamento que comentamos, o completar el suyo propio, identificando el fichero o tratamiento y el responsable de mismo, e incorporando las medidas de seguridad a implantar en relación con dicho tratamiento.

**El Título III** se ocupa de los derechos *-acceso, oposición, rectificación y cancelación-* de las personas en este ámbito. Según ha afirmado el **Tribunal Constitucional en su sentencia número 292/2.000** estos derechos constituyen el *haz de facultades que emanan del derecho fundamental a la protección de datos y sirven a la capital función que desempeña este derecho fundamental “garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer”*.

**Los Títulos IV a VII** permiten clarificar aspectos importantes para el tráfico ordinario, como la aplicación de criterios específicos a determinado tipo de ficheros de titularidad privada que por su trascendencia lo requerían *-los relativos a la solvencia patrimonial y crédito y los utilizados en actividades de publicidad y prospección*

*comercial-*, el conjunto de obligaciones materiales y formales que deben conducir a los responsables a la creación e inscripción de los ficheros, los criterios y procedimientos para la realización de las transferencias internacionales de datos y, finalmente la regulación de un instrumento *-el código tipo-* llamado a jugar cada vez un papel más relevante como elemento dinamizador del derecho fundamental a la protección de datos.

**El Título VIII** *-consta de IV capítulos; disposiciones generales –artículos 79 a 87-; el documento de seguridad -artículo 88-; medidas de seguridad aplicables a ficheros y tratamientos automatizados -artículos 89 a 104- y medidas de seguridad aplicables a los ficheros y tratamientos no automatizados -artículos 105 a 114-* regula un aspecto esencial para la tutela del fundamental derecho a la protección de datos; la seguridad.

Finalmente el **Título IX** se dedica a los procedimientos tramitados por la Agencia Española de Protección de Datos, se ha optado por normar exclusivamente aquellas especialidades que diferencian a los distintos procedimientos tramitados por la Agencia de las normas generales previstas en la **Ley 30/1992, de 26 de noviembre de Régimen Jurídico de la Administraciones Públicas y del procedimiento Administrativo Común** que actúa como derecho supletorio en esta materia.

A continuación trataremos los siguientes apartados:

- en primer lugar, el contenido del documento de seguridad que cada entidad deberá tener en el caso de tratar datos de carácter personal;
- en segundo lugar, la aplicación de los niveles de seguridad que corresponderán a las medidas de protección de datos de carácter personal; y
- en tercer y último lugar, las medidas aplicables a los ficheros y tratamientos automatizados, y no automatizados, atendiendo a los distintos niveles de seguridad, básico, medio y alto.

Con respecto al **documento de seguridad**, (art. 88), éste deberá contener como mínimo lo siguiente:

- 1) **Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.**
- 2) **Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento.**

- 3) Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.
- 4) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.
- 5) Procedimiento de notificación, gestión y respuesta ante las incidencias.
- 6) Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.
- 7) Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.

Cuando exista un tratamiento de datos por cuenta de terceros, el documento de seguridad deberá contener la identificación de los ficheros o tratamientos que se traten en concepto de encargado con referencia expresa al contrato o documento que regule las condiciones del encargo, así como de la identificación del responsable y del período de vigencia del encargo.

El documento de seguridad deberá mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los ficheros o tratamientos o, en su caso, como consecuencia de los controles periódicos realizados. En todo caso, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

Respecto a las **disposiciones generales es de resaltar la aplicación de los niveles de seguridad, y que son básico, medio y alto.**

Según lo anterior, *y tal y como se prevé legalmente, **Todos** los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de **nivel básico.***

Además de las medidas de nivel básico, deberán implantarse las medidas de **nivel medio** en los siguientes ficheros o tratamientos de datos de carácter personal:

- a) Los relativos a **infracciones administrativas o penales**.
- b) Aquellos cuyo funcionamiento se rija por el artículo 29 -prestación de servicios de información sobre solvencia patrimonial y crédito- de la Ley Orgánica 15/1.999, de 13 de diciembre.
- c) Aquellos de los que sean **responsables administraciones tributarias** y se relacionen con el ejercicio de sus potestades.
- d) Aquellos de los que **sean responsables las entidades financieras** para finalidades relacionadas con la prestación de servicios financieros.
- e) Aquellos de los **que sean responsables las entidades gestoras y servicios comunes de la Seguridad Social y las mutuas de accidentes de trabajo y enfermedades profesionales**.
- f) Aquellos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de **las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos**.
- g) Aquellos **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, con motivo del cumplimiento de deberes públicos

Además de las medidas de nivel básico y medio se implantarán medidas de **nivel alto** en los ficheros o tratamientos de carácter personal:

- a) **Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud, o vida sexual**, en caso de que los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o cuando 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 bastará con que se implante un nivel de seguridad básico.*

- b) Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.*
- c) Aquellos que contengan datos derivados de actos de violencia de género.*

En el ámbito de las medidas de seguridad aplicables a los **ficheros y tratamientos automatizados**, las medidas de seguridad de nivel básico contemplarán:

- 1) Las funciones y obligaciones del personal (art.89) con acceso a los datos de carácter personal y a los sistemas de información, estando claramente definidas y documentadas en el documento de seguridad. La persona responsable del fichero o del tratamiento informará a dicho personal de las normas de seguridad que afecten al desarrollo de sus funciones, así como de las consecuencias en que pudieran incumplir en caso de incumplimiento;
- 2) Registro de incidencias (art.90), en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas;
- 3) Control de acceso (art.91) a los usuarios, sólo a los recursos que precisen para la realización de sus funciones. La persona responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, así como los accesos autorizados para cada uno de ellos.
- 4) Gestión de soportes y documentos que contengan datos de carácter personal. (art.92).
- 5) Identificación y autenticación de los usuarios que intenten acceder al sistema de información y la verificación de que esté autorizado (art.93). Si el sistema de autenticación se basa en la existencia de contraseñas, habrá que asegurar su garantía al cambiarlas todos los

años, por lo menos una vez. Durante su vigencia, las contraseñas deberán ser almacenadas de forma ininteligible.

- 6) Copias de respaldo y recuperación. (art.94). Se deberán hacer semanalmente. La persona responsable del fichero hará cada seis meses, verificaciones la correcta realización de estas copias.

Respecto a las medidas de seguridad de nivel medio, contemplarán:

- 1) Un responsable de seguridad a designar en el documento de seguridad, encargado de coordinar y controlar las medidas definidas en el mismo. Este responsable es además del responsable del fichero y/o encargado del tratamiento, tal y como prevé este Reglamento. (art. 95)
- 2) Cada 2 años como mínimo se realizará una auditoria, interna o externa, tanto de los sistemas de información, como de las instalaciones de tratamiento y almacenamiento de datos. Los informes de esta auditoría serán analizados por el responsable de seguridad, quien elevará las conclusiones al responsable de fichero y/o encargado de tratamiento. (art.96)
- 3) En le ámbito de la gestión de soportes y documentos: registro de entrada y salida. Se adoptarán medidas para impedir la recuperación posterior de información de un soporte que vaya a ser desechado o reutilizado. Medidas que impidan la recuperación indebida de la información almacenada en un soporte que vaya a salir como consecuencia de operaciones de mantenimiento.
- 4) En le ámbito de la identificación y autenticación: Se establecerá mecanismos que permitan la identificación de forma inequívoca y personalizada de todo usuario y la verificación de que está autorizado. Límite de intentos reiterados de acceso no autorizado.
- 5) Control de acceso físico a los locales donde se encuentren ubicados los sistemas de información.
- 6) En le ámbito del Registro de incidencias: Registrar la realización de procedimientos de recuperación de los datos, persona que los ejecuta, datos restaurados y grabados manualmente. Autorización por escrito del responsable del fichero para su recuperación.

Respecto a las medidas de seguridad de nivel alto, se adoptarán en los siguientes campos:

- 1) Gestión y distribución de soportes: cifrado de datos en la distribución de soportes.
- 2) Copias de respaldo y procedimientos de recuperación en lugar diferente del que se encuentren los equipos.
- 3) Registro de usuario, hora, fichero, tipo de acceso y registro accedido. Control del responsable de seguridad. Informe mensual. Conservación de dos años.
- 4) Telecomunicaciones: la transmisión de datos será cifrada.

En el ámbito de las medidas de seguridad aplicables a los **ficheros y tratamientos no automatizados**, las **obligaciones comunes** en cuanto a las **medidas de seguridad de nivel básico** afectan al *alcance (artículo 79)*; a los *niveles de seguridad (artículo 80)*; al *encargado del tratamiento (artículo 82)*; a las *prestaciones de servicios sin acceso a datos personales (artículo 83)*; a la *delegación de autorizaciones (artículo 84)*; al *régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento (artículo 86)*; a los *ficheros temporales o copias de trabajo de documentos (artículo 87)*; al *documento de seguridad (artículo 88)*.

Igualmente corresponde al nivel básico de seguridad todo lo relativo a *las funciones y obligaciones del personal con acceso a los datos (artículo 89)*; al *registro de incidencias (artículo 90)*; al *control de acceso (artículo 91)* y a la *gestión de soportes y documentos (artículo 92)*.

Las medidas de seguridad aplicables a los ficheros y tratamientos no automatizados se completan con los **criterios de archivo que se adoptarán de conformidad con los previstos en su respectiva legislación (artículo 106)**; los **dispositivos de almacenamiento (artículo 107)** y la **custodia de los soportes (artículo 108)**.

Respecto a las **medidas de seguridad de nivel medio**, son las mismas que las del nivel básico, con dos adiciones, la primera que debe designarse un *responsable de seguridad (artículo 109)* y que *los ficheros sometidos a seguridad de nivel medio deben pasar, cada dos años, una auditoria -interna o externa- (artículo 110)*.



Las medidas de **seguridad de nivel alto**, son las mismas que las del nivel medio, con cuatro adiciones:

- El almacenamiento de la información (*artículo 111*).
- Copia o reproducción, bajo control de personal autorizado (*artículo 112*).
- El acceso a la documentación (*artículo 113*).
- Traslado de la documentación (*artículo 114*).