

Lo que interesa conocer sobre el
**Reglamento
de Protección de Datos**



Lo que interesa conocer sobre el Reglamento de Protección de Datos



Autores:

- **Emilio Gómez**
Abogado. Socio A&S Sampere
Bufete miembro de HISPAJURIS
- **Rosario Romero**
Abogada. A&S Sampere
Bufete miembro de HISPAJURIS



I. Introducción	5
II. Entrada en vigor. Plazo especial para los ficheros preexistentes	6
III. Disposiciones generales	8
III.1 Ámbito de aplicación	
III.2 Definiciones	
IV. Principios de protección de datos	9
IV.1 Principio de calidad	
IV.2 Principio de consentimiento	
IV.3 Principio de información	
V. Derechos de los interesados	12
VI. Disposiciones relativas a determinados ficheros de titularidad privada	13
VI.1 Ficheros de solvencia patrimonial y crédito	
VI.2 Tratamiento para actividades de publicidad y protección comercial	
VII. Obligaciones previas al tratamiento de los datos	16
VII.1 Inscripción de ficheros en el registro general de la AEPD	
VII.2 Transferencia internacional de ficheros	
VIII. Transferencia internacional de ficheros	17
IX. Códigos tipo.....	18
X. Medidas de seguridad en el tratamiento de datos de carácter personal.....	19
X.1 Cuestiones generales	
X.2 Niveles de seguridad	
X.3 Documentos de seguridad	
X.4 medidas de seguridad de ficheros y tratamientos automatizados	
X.5 Medidas de seguridad de ficheros y tratamientos no automatizados	
XI. Procedimientos tramitados por la AEPD.....	24
XII. El encargado del tratamiento	25
XIII. Conclusión	26
HispaJuris: servicios jurídicos en toda España.....	27
Relación de Bufetes miembros de HISPAJURIS	28



Introducción

El día 21 de Diciembre de 2007 fue aprobado el Real Decreto 1720/2007 (en adelante, el RDLOPD), de desarrollo de la Ley Orgánica 15/1999, de 13 de Diciembre, de protección de datos de carácter personal (en adelante, la LOPD), el cual entró en vigor el pasado 18 de Abril de 2008.

La nueva norma persigue, junto con la LOPD, la protección de los derechos fundamentales de las personas físicas frente a las injerencias en los mismos causadas por el acopio y tratamiento masivo de datos de carácter personal.

Para ello el legislador aglutina la normativa vigente hasta este momento, a la que incorpora la casuística y experiencia de todos los agentes implicados en la aplicación y puesta en marcha de la LOPD: empresas, autónomos, particulares, incluidas las Resoluciones de la Agencia Española de Protección de Datos y las Sentencias y Autos de los Tribunales de Justicia.

Se derogan expresamente las siguientes normas (Disposición Derogatoria Única):

A. Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, la conocida como LORTAD (en adelante, RD 1332/94).

B. 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 (en adelante, RD 994/99).

C. Todas las normas de igual o inferior rango que contradigan o se opongan a lo dispuesto en el nuevo Reglamento, RD 1720/2007.

En el presente informe pretende dar a conocer las novedades y consecuencias prácticas que tiene la aprobación y entrada en vigor del RDLOPD.

Entrada en vigor. Plazo especial para ficheros preexistentes

II.1.- El RDLOPD entró en vigor el pasado 18 de Abril de 2008 (Disposición Final Segunda); por lo que a partir de esta fecha, su cumplimiento será de plenamente exigible.

No obstante, en sus Disposiciones transitorias se establece un período transitorio para los ficheros que ya existían a la fecha de su entrada en vigor; fijándose los plazos en los que los Responsables del fichero o encargados de tratamiento deberán adoptar las medidas y llevar a cabo las actuaciones necesarias actualizar su situación a la nueva normativa.

A) Ficheros que existan a la entrada en vigor del RDLOPD (ficheros automatizados):

Existe un plazo general de un (1) año para la adopción de todas aquellas medidas o actuaciones que no estaban previstas por la anterior normativa.

En idéntico plazo de un (1) año deben adoptar las medidas de seguridad de nivel medio

- Los ficheros de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social, y se relacionen con el ejercicio de sus competencias.
- Los ficheros de los que sean responsables las Mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social. Adicionalmente, se establecen plazos espe-

cíficos para los ficheros que contengan datos derivados de actos de violencia de género y 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 de los datos de tráfico y a los datos de localización.

B) Ficheros que existan a la entrada en vigor del RDLOPD (no automatizados):

Se fijan los siguientes plazos para su adecuación a la nueva regulación:

NIVEL DE SEGURIDAD	PLAZO DE IMPLANTACIÓN
Básico	1 año
Medio	18 meses
Alto	2 años

C) En el plazo de un (1) año desde la entrada en vigor del Reglamento, aquellos sectores de actividad que tengan inscritos (o estén adheridos a) Códigos Tipo deberán notificarse a la Agencia Española de Protección de Datos las modificaciones que resulten necesarias.



Disposiciones generales

III.1 ÁMBITO DE APLICACIÓN.

El RDLOPD será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento y toda modalidad de uso posterior de estos.

Como importante novedad, se excluyen del ámbito de aplicación el tratamiento y ficheros que contengan únicamente:

- i) Datos de personas jurídicas.
- ii) Datos profesionales de personas físicas, siempre y cuando dichos datos queden limitados a nombre, apellidos, funciones, tareas o cargo de la persona física, su dirección postal o electrónica, teléfono y fax profesionales (las conocidas como "tarjetas de visitas").
- iii) Datos relativos a empresarios individuales, cuando hagan referencia a ellos en calidad de profesionales ("datos de trabajadores autónomos").
- iv) Datos de personas fallecidas.

III.2. DEFINICIONES.

El artículo 5 del RDLOPD recoge una serie de definiciones necesarias para entender y poder aplicar correctamente esta normativa.

Dada su extensión, dicho listado de definiciones se acompaña al presente informe como **Anexo I** sin perjuicio de resaltar desde ahora las siguientes pautas generales:

- Las definiciones de afectado, consentimiento o cesión de datos no han sufrido ninguna modificación.
- Las definiciones de fichero, dato de carácter personal y la de encargado del tratamiento no han sido objeto de modificación, pero han sido desarrolladas con mayor profundidad, lo que facilita su comprensión.
- Aparecen definiciones que hasta el momento no había sido recogidas en ninguna norma, sin perjuicio de que fueran de utilización habitual: datos de carácter personal relacionados con la salud, tercero, exportador de datos, importador de datos, documento, perfil de usuario o transmisión de documentos.
Quedan así delimitados y detallados con mayor profundidad los conceptos utilizados a lo largo del articulado de la normativa vigente en materia de protección de datos.

Principios de protección de datos

IV.1.- PRINCIPIO DE CALIDAD.

En virtud del principio de calidad, los datos deben ser tratados de forma leal y lícita, y sólo podrán ser objeto de tratamiento los datos adecuados, pertinentes y no excesivos en relación con la finalidad determinada para la que fueron recabados.

El RDLOPD introduce las siguientes novedades:

- i) La presunción de exactitud de los datos cuando los mismos son facilitados directamente por el interesado.
- ii) Se establece un plazo de 10 días para efectuar las cancelaciones o sustituciones que procedan cuando los datos sean inexactos o incompletos.
- iii) En el caso en el que los datos haya sido objeto de cesión, en el mismo de diez (10) días deberá comunicarse la cancelación o rectificación al cesionario, quien a su vez cuenta con idéntico plazo para efectuar las cancelaciones o rectificaciones oportunas.

IV.2.- PRINCIPIO DE CONSENTIMIENTO.

Los datos de carácter personal sólo pueden ser objeto de tratamiento si el interesado ha prestado su consentimiento para ello, salvo las excepciones legalmente previstas en la LOPD.

Asimismo, con una exhaustividad hasta ahora inexistente, se regula la forma en la que debe recabarse el consentimiento, admitiendo tanto el consentimiento expreso como el tácito (art. 14). El consentimiento tácito ha sido una de las cuestiones más debatidas antes de la aprobación del RDLOPD, se venía utilizando ya en determinadas situaciones, ahora obtiene el respaldo legal.

Como novedad, el RD 1720/2007 detalla el modo en el que debe solicitarse el consentimiento para que el mismo sea válido, aún siendo prestado de forma tácita:

- i) Debe facilitarse al interesado la información oportuna sobre el tratamiento o serie de tratamientos, con delimitación de la finalidad para la que se recaban los datos, así como el resto de condiciones que concurran en el tratamiento.
- ii) Debe concederse al interesado un plazo de 30 días para manifestar su negativa al tratamiento, advirtiéndole que en caso contrario se entenderá que consiente el tratamiento.

Adicionalmente, cuando se pretenda recabar el consentimiento tácito mediante la remisión de comunicaciones postales o electrónicas, el remitente (responsable del fichero o encargado del tratamiento) ha de poder conocer si la co-



municación ha sido objeto de devolución, pues, en este caso, no podrá tratar los datos.

El Responsable del fichero debe facilitar al interesado un medio sencillo y gratuito para mostrar su oposición, entendiendo que serán medios válidos los siguientes:

- Envío prefranqueado al responsable del tratamiento.
- Número de teléfono gratuito (línea 900)
- Servicios de atención al cliente.

Cuando se recabe el consentimiento en el ámbito de una relación contractual, de cualquier naturaleza, y el responsable del fichero pretenda tratar los datos con alguna finalidad que no guarde relación con la meramente contractual (por ejemplo remitirse información promocional de la empresa) debe habilitarse un procedimiento para que el interesado pueda manifestar de forma expresa su negativa a la finalidad accesoria; se entenderá cumplida esta condición cuando se permita la interesado marcar una casilla claramente visible en el contrato que se celebra con el responsable del fichero.

El titular de los datos podrá en cualquier momento revocar el consentimiento prestado.

Como novedad más significativa la norma aprobada establece como medios idóneos para revocar el consentimiento:

Medios que se consideran ajustados al RDLOPD: el envío prefranqueado al responsable del tratamiento o la llamada a un número telefónico gratuito o a los servicios de atención al público que el responsable del tratamiento hubiera establecido.

Medios que no se considera ajustados al RDLOPD: entre otros medios, envío de carta certificada o semejantes, la utilización de servicios de telecomunicaciones que impliquen tarificación adicional al afectado o cualesquiera otros medios que impliquen un coste adicional para el afectado.

Se introduce la regulación del consentimiento prestado por menores de edad, cuestión que había sido objeto de interpretación por parte de la Agencia Española de Protección de Datos a través de diversas resoluciones; diferenciando:

- A) Consentimiento prestado por mayores de catorce años: será válido, salvo en aquellos supuestos en los que la Ley exija la asistencia de los titulares de la patria potestad o tutela.
- B) Consentimiento prestado por menores de catorce años: para que sea válido debe ser ratificado por el consentimiento de los padres o tutores.

En todo caso, se prohíbe recabar del menor, sin contar con el consentimiento de los padres o tutores, datos que permitan obtener información sobre los demás miembros del grupo familiar, o sobre las características del mismo (actividad profesional, información económica); sin perjuicio de que sí pueden recabarse los datos de identidad y dirección del padre, madre o tutor, con la única finalidad de obtener la autorización para el tratamiento de la información del grupo familiar.

Se impone al Responsable del Fichero la en muchas ocasiones difícil tarea de comprobar de modo efectivo la edad del menor y la autentici-

dad del consentimiento prestado por los padres o tutores; lo que podrá originar serios problemas prácticos en la aplicación de la norma por algunos sectores empresariales.

IV. 3.- PRINCIPIO DE INFORMACIÓN.

El RDLOPD exige la conservación del documento o medio a través del cual se ha informado al interesado, entre otros aspectos, sobre la existencia de un o varios ficheros, la identidad del responsable del fichero, la finalidad del tratamiento y los derechos que ostenta.

Este documento o medio deberá conservarse a fin de acreditar el cumplimiento del deber de informar.

Los responsables del fichero deberán habilitar un procedimiento para conservar los documentos (ya sean en soporte papel o automatizado) en los que se facilita la información al interesado; dejándose libertad al Responsable, para determinar dónde y cómo se conservarán esos documentos, pues no se indica previsión alguna al respecto.

En el artículo 19 se establece que no existe cesión de datos cuando se modifica el responsable del fichero como consecuencia de una operación de fusión, escisión global de activos y pasivos, aportación o transmisión de negocio o rama de actividad empresarial u operaciones similares; lo cual resuelve importantes problemas prácticos y agiliza el trasvase de información entre las empresas.

En el caso de tratarse de información dirigida a menores de edad, ésta ha de ser comprensible, por lo que debe utilizarse un lenguaje o

expresiones claras y entendibles en atención a las características de los menores a los que se dirige la información (artículo 13 RDLOPD).



Derechos de los interesados

El RDLOPD dota de claridad la regulación de los derechos de los afectados en materia de protección de datos, toda vez que recoge soluciones prácticas tanto para los interesados en el momento de ejercitar sus derechos como para los responsables de ficheros cuando deben dar satisfacción al derecho o denegar el mismo.

El Reglamento desarrolla los siguientes aspectos de los derechos del interesado:

- a) Las condiciones generales para el ejercicio de los derechos: tienen carácter personalísimo, son derechos independientes entre sí, y para su ejercicio se debe facilitar al interesado un medio sencillo y gratuito.
- b) El procedimiento que debe seguir el interesado para ejercitar su derecho.
 - i) Contenido mínimo de la comunicación dirigida al Responsable del fichero para ejercitar el derecho/s.
 - ii) Documentos mínimos que deben acompañar a la comunicación.
- c) El procedimiento que debe seguir el responsable del fichero para dar cumplimiento o satisfacer el derecho, o en su caso, en los supuestos que proceda, denegar el ejercicio del derecho:
 - i) En todo caso (se tengan datos o no del afectado) se debe contestar al requerimiento.
 - ii) Ante una comunicación defectuosa, debe solicitarse la subsanación.
 - iii) El responsable del fichero estará obligado a acreditar que ha dado cumplimiento al derecho.
 - d) El procedimiento para el caso en el que el derecho se ejercite ante un encargado del tratamiento, no ante el propio responsable del fichero:

Deberá darse traslado de la solicitud/comunicación al responsable del fichero.

Disposiciones relativas a determinados ficheros de titularidad privada

Ya en la LOPD venían regulados específicamente algunos ficheros de titularidad privada que precisaban de un tratamiento jurídico complejo, bien por la naturaleza de los datos que contienen, bien por el volumen de datos que contiene o la injerencia que un uso inadecuado de los mismos podría suponer en la esfera de la privacidad, o incluso intimidad de los interesados. El RDLOPD desarrolla ahora la regulación de estos ficheros:

VI.1. FICHEROS DE SOLVENCIA PATRIMONIAL Y CRÉDITO.

Son los conocidos como “ficheros de morosos”. Las novedades más significativas en la regulación de estos ficheros son:

- a) Exigencia de informar al interesado con carácter previo a la inclusión de sus datos en el fichero:
 - i) En el momento de celebración del contrato.
 - ii) En el requerimiento de pago de la deuda.
- b) El procedimiento para la notificación al interesado de que sus datos han sido incluidos en el fichero.
 - i) Se debe notificar en los 30 días desde el registro en el fichero.
 - ii) Una notificación por cada deuda concreta y determinada.
 - iii) El medio a través del cual se notifique al interesado debe ser fiable, auditable e indepen-

diente, y que ha de permitir conocer si ha sido objeto de devolución.

- c) El modo y plazo en el que pueden conservarse los datos en este tipo de ficheros.
 - i) Solo se podrán tratar datos veraces.
 - ii) Obligación de cancelar de los datos:
 1. Cuando la deuda se haya pagado o cumplido la obligación.
 2. Transcurridos seis años desde el registro de los datos.
 - d) Sólo podrán acceder a los datos contenidos en los ficheros de solvencia patrimonial y crédito terceros con la finalidad de enjuiciar la solvencia económica del interesado.
- ## VI.2. TRATAMIENTO PARA ACTIVIDADES DE PUBLICIDAD Y PROSPECCIÓN COMERCIAL.
- Dentro de este apartado se incluyen:
- i) Los ficheros y tratamientos de los responsables cuya actividad sea la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial o actividades análogas.
 - ii) Los ficheros y tratamientos de aquellos responsables, que teniendo una actividad empresarial distinta a las enunciadas en el apartado I), desarrollan, por sí mismos o a través de terceros, estas actividades para comercializar sus propios productos o servicios.



Recordemos que la LOPD prevé que los responsables del fichero que desarrollen tratamiento de datos para actividades de publicidad y prospección comercial sólo podrán utilizar nombre y direcciones u otros datos análogos cuando los mismos se encuentren en uno de los dos supuestos siguientes:

- i) Cuando figuren en fuentes accesibles al público.
- ii) Cuando hayan sido facilitados por los propios interesados u obtenidos con su consentimiento.

Este segundo supuesto es desarrollado por el Reglamento, que expresamente exige:

- 1 Que el consentimiento se haya prestado para finalidades determinadas, explícitas y legítimas con la actividad de publicidad o prospección comercial; y,
- 2 Que se haya informado a los interesados sobre los sectores específicos y concretos de actividad respecto de los cuales podrán recibir información.

En consecuencia con lo expuesto, y a la vista de las disposiciones del RD 1720/2007, no serán válidas las cláusulas informativas a través de las cuales se solicita al interesado su consentimiento para “remitir información de su interés”, debiendo especificarse, al menos, los sectores o actividades empresariales de los cuales se remitirá información.

Ello supondrá la necesidad de verificar las cláusulas informativas utilizadas en el tráfico mercantil, e introducir las oportunas modificaciones en las mismas, para adecuarlas a lo dispuesto en la normativa vigente.

Adicionalmente, se ha desarrollado un supues-

to que en la práctica no está exento de complejidad, cual es el tratamiento de datos en campañas publicitarias realizadas, bien directamente por los responsables del fichero, bien a través de empresas especializadas. En este supuesto, el artículo 46 del Reglamento distingue los supuestos en los que la empresa que encarga o contrata la campaña de publicidad es responsable del fichero, de aquellos otros en los que es encargada del tratamiento. Así, en caso de que una entidad contrate o encomiende a terceros la realización de una determinada campaña publicitaria de sus productos o servicios, encomendándole el tratamiento de determinados datos, se aplicarán las siguientes normas (art. 46):

- Cuando los parámetros identificativos de los destinatarios de la campaña sean fijados por la entidad que contrate la campaña, ésta será responsable del tratamiento de datos.
- Cuando los parámetros fueran determinados únicamente por la entidad o entidades contratadas, dichas entidades serán responsables del tratamiento.
- Cuando en la determinación de los parámetros intervengan ambas entidades, serán ambas responsables del tratamiento.

Por otra parte, se regulan las conocidas hasta ahora como “listas Robinson” o ficheros de exclusión de envío de comunicaciones comerciales, los cuales han sido muy poco utilizados por los particulares, y que permiten discriminar a voluntad del interesado aquella información que deseamos nos remitan, y la que no deseamos recibir (art 49 RDLOPD).

Obligaciones previas al tratamiento de los datos

VII.1.- INSCRIPCIÓN DE FICHEROS ANTE EL REGISTRO GENERAL DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS.

Se mantiene la obligación prevista en el artículo 26 de la LOPD, según el cual con carácter previo a la creación de un fichero que contenga datos de carácter personal, el mismo debe ser notificado al Registro General de la Agencia Española de Protección de Datos.

En el caso de los ficheros de titularidad privada, el Reglamento no indica con qué plazo de antelación a la creación debe efectuarse la notificación al Registro, lo que podría generar cierta inseguridad jurídica a los responsables del fichero. En todo caso, la notificación debe ser previa a la creación.

El procedimiento administrativo para la inscripción de los ficheros, finalizará mediante una Resolución del Director de la Agencia Española de Protección de Datos, a propuesta del Registro General de Protección de Datos, la cual contendrá entre otra, la siguiente información:

- Código de Inscripción,
 - Identificación del Responsable del Fichero,
 - Identificación del Fichero,
 - Descripción de la finalidad y usos previstos,
- Medidas de seguridad.

VII.2.- NOTIFICACIÓN DE LA MODIFICACIÓN O SUPRESIÓN DE FICHEROS.

A diferencia de lo que disponía el artículo 8 del Real Decreto 1332/1994, de 20 de junio (el cual ha sido expresamente derogado por el Reglamento), el artículo 58 del RDLOPD obliga a los responsables del fichero a notificar las modificaciones y/o supresiones de los ficheros con carácter previo a que se produzcan, si bien tampoco indica el plazo de antelación con el que debe realizarse.



Transferencia internacional de datos

Se mantiene como norma general la necesidad de contar con autorización del Director de la Agencia Española de Protección de Datos para realizar transferencias internacionales de datos, salvo en los siguientes supuestos:

- A) Que nos encontremos ante una de las excepciones legalmente previstas.
- B) Que la transferencia se efectúe a un Estado que ofrezca un nivel adecuado de protección de datos.

En todo caso, el responsable del fichero debe comunicar al Registro General de Protección de Datos la transferencia internacional de datos que va a efectuarse.

La novedad más significativa la encontramos en el artículo 70.4 del Reglamento, el cual prevé que podrá otorgarse la autorización para la transferencia de datos en el seno de grupos multinacionales de empresas cuando hubiesen sido adoptadas normas o reglas internas, vinculantes para las empresas que integran el grupo, y en las que al menos se contengan medidas que garanticen:

- a) El respeto a la protección de la vida privada y el derecho fundamental a la protección de datos;
- b) El cumplimiento de los principios previstos en la LOPD;

- c) El ejercicio de los derechos reconocidos por la LOPD y desarrollados por el Reglamento.

Con ello, se facilita el trasvase de información entre la empresa matriz ubicada fuera del territorio de la Unión Europea, y la filial ubicada en España.

Códigos tipo

Los Código Tipo ya venían definidos en el art. 2.3 de la LOPD como aquellos acuerdos sectoriales, convenios administrativos o decisiones de empresa formulados por los responsables de ficheros, así como por organizaciones en que estos se agrupen, que recogen entre otros aspectos, condiciones de organización, normas de seguridad, obligaciones de los implicados en el tratamiento o uso de datos, así como garantías para el ejercicio de los derechos y normas para el pleno respeto de los principios en materia de protección de datos.

La regulación de los Códigos Tipo estaba reducida a tres preceptos (art. 32 de la LOPD, arts. 9 y 10 del Real Decreto 1332/1999), pese a su indudable utilidad para dar a conocer a los responsables del fichero integrados en un determinado sector, las obligaciones que tienen en materia de protección de datos, y mediante los cuales adquieran un compromiso en el tratamiento de los datos que vaya más allá del mero cumplimiento de la misma.

Pese a las ventajas que tiene el uso de los Códigos Tipo, llama poderosamente la atención que desde la entrada en vigor de la LOPD, únicamente se hayan aprobado y publicado once (11) Códigos.

Los Códigos Tipo que deben contener, entre otros aspectos:

- Ámbito de aplicación.
- Previsiones específicas para la aplicación en el sector de los principios en materia de protección de datos.
- Estándares homogéneos para el cumplimiento de la normativa vigente en materia de protección de datos por los adheridos a los mismos.
- Acciones formativas de las empresas.
- Cláusulas tipo para la obtención del consentimiento e información de los interesados.
- Procedimiento de supervisión independientes para la garantizar su cumplimiento.
- Régimen sancionador adecuado, eficaz y disuasorio.
- Relación de adheridos.



Medidas de seguridad en el tratamiento de datos de carácter personal

La Exposición de Motivos del RDLOPD nos desvela cuál es el objetivo en cuanto a las medidas de seguridad:

"(...) ser particularmente riguroso en la atribución de los niveles de seguridad, en la fijación de las medidas que corresponde adoptar en cada caso y en la revisión de las mismas cuando ello resulte necesario. Por otra parte ordena con mayor precisión el contenido y las obligaciones vinculadas al mantenimiento del documento de seguridad. Además, se ha pretendido regular la materia de modo que contemple las múltiples formas de organización material y personal de la seguridad que se da en la práctica. (...)".

A nuestro parecer, y siempre salvo mejor criterio u opinión, no todos los objetivos se han cumplido, a pesar del tiempo y esfuerzo invertido en la elaboración y publicación del Reglamento.

X.1.- CUESTIONES GENERALES.

Se pretende resolver cuestiones prácticas que se han planteado a los responsables del fichero y encargados del tratamiento en el momento de aplicar las medidas de seguridad previstas reglamentariamente a la realidad de los sistemas de información y de la propia organización

empresarial; así, se da respuesta a las siguientes cuestiones que carecían de regulación específica:

- ¿Es posible la delegación de autorizaciones por parte del Responsable del Fichero o encargado del tratamiento?
- Sí es posible, el RDLOPD.
- ¿El Documento de Seguridad debe ser único? ¿Es posible elaborar tantos documentos de seguridad como ficheros tengamos?.
- El responsable del fichero podrá elaborar uno o varios documentos de seguridad.
- ¿Debe nombrarse un único Responsable de Seguridad ¿Es posible nombrar un Responsable de Seguridad por cada fichero o conjunto de ficheros?
- El responsable del fichero podrá nombrar uno o varios Responsables de Seguridad.

X.2.- NIVELES DE SEGURIDAD

El RD 1720/2007 mantiene los tres niveles de seguridad ya previstos en la normativa anterior: Básico, Medio y Alto.

A) Nivel Básico.

La novedad más significativa se encuentra en el aplicación (interpretación) conjunta de los apartados 5 y 6 del artículo 81, previéndose que se encuentran en el Nivel Básico los fiche-

ros de nómina/personal/RRHH, que contengan datos económicos de nómina, , y que además pudieran contener:

- Datos de afiliación sindical, con el único y excluso fin de realizar el descuento sindical; y/o,
- Datos de salud, referidos únicamente a grado de discapacidad o simple declaración de discapacidad o invalidez, con el único y exclusivo fin de satisfacer las obligaciones del responsable del fichero (por ejemplo, la comunicación a los Organismos competentes de la Seguridad Social)

Es decir, el Reglamento aclara la discusión doctrinal acerca del nivel de seguridad de los ficheros de nómina, habilitando la regulación precisa para que los mismos, en general, puedan encuadrarse en el nivel básico de seguridad.

Asimismo, Nivel Básico de Seguridad se aplicará a los ficheros o tratamientos que contengan, de forma incidental o accesorio, datos especialmente protegidos (tales como datos de religión, creencia, ideología, origen racial o salud); siempre y cuando los ficheros sean no automatizados y no guarden relación con la finalidad del fichero.

Los términos “*de forma incidental o accesorio*”, son excesivamente genéricos, provocando inseguridad jurídica, y nos hace plantearnos las siguientes cuestiones:

- 1 ¿Qué debemos entender por incidental o accesorio?
- 2 Dado que son datos especialmente protegidos que afectan de forma directa a la

intimidad de las personas ¿No deberían tener en todo momento la protección de nivel alto prevista en el art. 81.3 del Reglamento?

- 3 ¿Cómo es posible que se mantenga en un fichero un dato que no guarda relación con la finalidad del tratamiento? ¿No se contraviene con ello el principio de calidad de los datos?

Posiblemente esta cuestión originará en su aplicación una gran problemática e incluso litigiosidad.

B) Nivel Medio.

Se mantienen en este Nivel de Seguridad los ficheros relativos a la comisión de infracciones administrativas o penales, los ficheros de prestación de servicios de información sobre solvencia patrimonial y crédito, y aquellos ficheros que contengan un conjunto de datos que ofrezcan una definición de las características o personalidad del interesado y que permitan evaluar determinados aspectos de su personalidad o comportamiento.

Se incluyen dentro del nivel medio de seguridad (artículo 81.2 c) los ficheros de los que sean responsables las Administraciones Tributarias y se relacionen con el ejercicio de sus potestades tributarias; con ello se aclara la interpretación que debía darse al término “Hacienda pública” incluido en el artículo 4.2 del derogado Real Decreto 999/1994, y que había sido objeto de diversas interpretaciones.

Asimismo, se incluyen dentro del Nivel Medio:



- Los ficheros de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros.
- Los ficheros de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social, y se relacionen con el ejercicio de sus competencias.
- Los ficheros de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

C) Nivel Alto.

Se mantienen en este nivel de seguridad los ficheros que contengan datos especialmente protegidos (ideología, religión, creencia, origen racial, salud o vida sexual) y aquellos ficheros que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas.

Igualmente, en el Nivel Alto de seguridad se incluyen aquellos ficheros que contengan datos derivados de actos de violencia de género.

X.3.- DOCUMENTO DE SEGURIDAD.

El artículo 88 del Reglamento determina el contenido mínimo que ha de tener el Documento de Seguridad, como reproducción casi literal de lo dispuesto en el artículo 8 del derogado del Real Decreto 994/1999.

El Documento de Seguridad deberá contener, como mínimo:

- Las medidas necesarias para el transporte, destrucción, o en su caso, reutilización de soportes y documentos.
- La identificación del/los responsable/s de seguridad; y

- Los controles periódicos para verificar el cumplimiento del documento de seguridad.

Como novedad, se obliga a los Encargados del Tratamiento a incluir en sus Documentos de Seguridad la identificación de los ficheros y tratamientos que manejen bajo la condición de encargados, indicando, entre otros aspectos, los datos del responsable del fichero y el período de vigencia del encargo.

Asimismo, el Responsable del Fichero hará constar en su Documento de Seguridad la existencia de uno o varios encargados del tratamiento, cuando los ficheros se encuentren ubicados en los sistema de información del encargado.

X.4.- MEDIDAS DE SEGURIDAD APLICABLES A FICHEROS Y TRATAMIENTOS AUTOMATIZADOS.

X.4.A.- MEDIDAS DE SEGURIDAD DE NIVEL BÁSICO.

X.4.A.1.- Controles de acceso.

Cuando personal ajeno al Responsable del Fichero tenga acceso a los recursos, deberán someterse a las mismas condiciones y obligaciones en materia de seguridad que los usuarios.

X.4.A.2.- Gestión de soportes.

Se mantiene la obligación de etiquetar los soportes, a fin de poder identificarlos, inventariarlos y conocer la información que contienen; salvo que las características del soporte imposibiliten el cumplimiento de esta obligación, en cuyo caso, debe reflejarse y motivarse en el Documento de Seguridad.

X.4.A.3.- Identificación y autenticación.

Como novedad más significativa, se establece una periodicidad máxima de validez de las contraseñas, que en ningún caso podrá ser superior a un (1) año.

X.4.A.4.- Copias de respaldo y recuperación.

Se introducen dos novedades:

- a) El establecimiento de un plazo mínimo de realización, que en ningún caso puede ser superior a una (1) semana.
- b) La obligación de verificar cada seis (6) meses el procedimiento de realización de copias de respaldo y recuperación.

X.4.B.- MEDIDAS DE SEGURIDAD DE NIVEL MEDIO.

X.4.B.1.- Responsable de Seguridad.

Se permite expresamente la designación de uno o varios Responsables de Seguridad.

Como cuestión que siempre ha preocupado a las personas designadas como Responsables de Seguridad, se aclara que esta designación no supone exoneración de la responsabilidad que corresponde al responsable del fichero o encargado del tratamiento.

X.4.B.2.- Auditoría.

El apartado de auditoría no introduce grandes novedades, se mantiene la obligación de realizar una auditoría bianual, y se introduce, con carácter extraordinario, la obligación de realizar una auditoría siempre que se realicen modificaciones sustanciales en el sistema de información.

X.4.B.3.- Gestión de soportes y documentos, Identificación y Autenticación, Control de acceso físico y Registro de incidencias.

Estas medidas de seguridad no han sufrido cambios, manteniéndose en su integridad.

X.4.C.- MEDIDAS DE SEGURIDAD DE NIVEL ALTO.

X.4.C.1.- Registro de accesos.

Se mantiene la obligación de disponer de un Registro de Accesos, excepto en los siguientes casos:

- a) Que el responsable del fichero o tratamiento sea una persona física.
- B) Que el responsable del fichero o tratamiento garantice que únicamente él tiene acceso y trata los datos personales.

En el Documento de Seguridad debe detallarse la concurrencia de las antedichas circunstancias.

X.5.- MEDIDAS DE SEGURIDAD APLICABLES A FICHEROS Y TRATAMIENTOS NO AUTOMATIZADOS (FICHEROS EN SOPORTE PAPEL).

Se trata posiblemente de la novedad más esperada y significativa del presente Reglamento, dado que hasta este momento, si bien esta categoría de ficheros o tratamientos se encontraban dentro del ámbito de aplicación general de la normativa vigente en materia de protección de datos, carecíamos de una guía legal para determinar las medidas de seguridad que debían implantarse en este tipo de ficheros.

Se extienden a los ficheros no automatizados aquellas mismas medidas que la norma prevé para los automatizados, entre ellas, elaborar e incluir en el Documento de Seguridad los siguientes aspectos:



- A) Funciones y obligaciones del personal
- B) Registro de incidencias.
- C) Control de accesos.
- D) Gestión de soportes.
- E) Auditoría.

Adicionalmente, dada su especificidad, se prevén como obligaciones adicionales para los ficheros y tratamientos no automatizados (ficheros en soporte papel):

A) Criterios de archivo:

En cada caso se atenderá a la legislación específica.

En defecto de legislación específica, el criterio utilizado deberá garantizar:

- 1 La conservación de lo documentos.
- 2 La localización de la información.
- 3 La consulta de la información.
- 4 El ejercicio de los derechos por parte de los interesados.

B) Obligación de implantar mecanismos que obstaculicen la apertura de los ficheros.

C) Obligación de establecer medidas para la custodia, almacenamiento y acceso a la información cuando no se encuentre archivada.

Los archivadores que contengan datos que por su naturaleza se encuentren en el nivel alto de seguridad deberán ubicarse en áreas restringidas y protegidas con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente; y si esto no fuera posible, se adoptarán medidas alternativas, dejando constancia de ello en el Documento de Seguridad.

D) Traslado de la documentación.

Deben adoptarse medidas para:

- 1 Impedir el acceso a la documentación.
- 2 Impedir la manipulación de la documentación.

Procedimientos tramitados por la Agencia Española de Protección de Datos

Se recogen en una única norma todos los procedimientos administrativos seguidos por la Agencia Española de Protección de Datos, ya sean de oficio o a instancias de parte.

La descripción tan prolija de cada uno de estos procedimientos excede del ámbito del presente informe, por lo que, sin perjuicio del esquema que a continuación realizamos, remitimos su estudio a las situaciones individualizadas que se pudieran presentar.

XI.1.- Procedimiento de tutela de los derechos de acceso, rectificación, cancelación y oposición.

XI.2.- Procedimientos relativos al ejercicio de la potestad sancionadora.

XI.3.- Procedimientos relacionados con la inscripción o cancelación de ficheros:

XI.3.A.- Procedimiento para inscripción de la creación, modificación o supresión de ficheros.

XI.3.B.- Procedimiento de cancelación de oficio de ficheros inscritos.

XI.4.- Procedimientos relacionados con la transferencia internacional de datos:

XI.4.A.- Procedimiento de autorización de transferencias internacionales de datos.

XI.4.B.- Procedimiento de suspensión temporal de transferencias internacionales de datos.

XI.5.- Procedimiento de inscripción de códigos tipo.

XI.6.- Otros procedimientos tramitados por la Agencia Española de Protección de Datos.

XI.6.A.- Procedimiento de exención del deber de información al interesado.

XI.6.B.- Procedimiento para la autorización de conservación de datos para fines históricos, estadísticos o científicos.



Encargado del tratamiento

Con carácter previo a la aprobación del RDLOPD, la regulación del encargado del tratamiento era muy parca, limitándose a lo dispuesto en el artículo 12 de la LOPD; sin embargo desde el punto de vista empresarial es una figura frecuentemente utilizada, y que por tanto ha planteado múltiples problemas en su aplicación práctica, por lo que era imprescindible su desarrollo reglamentario.

Las novedades más significativas en la regulación del encargado del tratamiento son:

- A) Se regula la subcontratación de los servicios encomendados al encargado del tratamiento.
- B) Se regula la conservación de los datos por el encargado del tratamiento una vez cumplida la prestación de servicios encomendada.
- C) La referencia de la existencia del encargado del tratamiento en el Documento de Seguridad, a fin de que los datos sean tratados conforme al nivel de seguridad adecuado, con independencia de que los mismos se encuentren en las instalaciones o sistemas de información del Responsable o del encargado del tratamiento.

En este caso, con un criterio que entendemos práctico y acertado, el RDLOPD ha recogido y aglutinado las diversas resoluciones interpreta-

doras de la AEPD y de los Tribunales de Justicia, proporcionando algo más de seguridad en materia de Protección de Datos; pero sin resolver algunas cuestiones que continúan siendo objeto de interpretación.

Conclusión

XII

El RD 1720/2007 viene a completar una regulación largamente esperada, que por su brevedad y complejidad había dejado a la interpretación numerosos aspectos esenciales para su aplicación práctica, lo que ha venido generando una grave inseguridad jurídica para todos los interlocutores implicados.

El estricto régimen sancionador (recordemos que el establecido en España es uno de los más estrictos de la Unión Europea) y la interpretación estricta de la normativa vigente en materia de protección de datos que se está realizando por parte de la Agencia Española de Protección de Datos, hacía necesaria la aprobación de una norma que aclarase, desarrollase y delimitase las previsiones de la LOPD.

Como sucede habitualmente, este tipo de desarrollo reglamentario impone nuevas exigencias para los obligados a cumplir la normativa (principalmente empresas y Organismos Públicos); lo cual hará necesario verificar y comprobar que la política de Protección de Datos se ajusta en cada caso a la nueva regulación legal.

El presente informe se emite bajo la condición de mejor criterio o parecer fundado en Derecho.



Hispajuris: servicios jurídicos en toda España

Hispajuris constituye la red de despachos más grande de España y una de las mayores entidades prestadoras de servicios jurídicos globales multidisciplinares, que ofrece una amplia cobertura territorial gracias a los 45 despachos integrados, todos ellos bufetes locales líderes. Hispajuris actúa, así, como un despacho global en el mercado nacional de servicios jurídicos.

LOS DESPACHOS HISPAJURIS

- Despachos locales líderes en su territorio y/o especialidad.
- Prestigio reconocido.
- Formados por abogados con una dilatada experiencia profesional.
- Mínimo de 10 años de ejercicio.
- Orientación al cliente: preocupación por su realidad y sus necesidades.
- Niveles de calidad exhaustivos.
- Arrraigados, con conocimiento del entorno.

Todos y cada uno de los despachos de Hispajuris cumplen unos mismos requisitos que hacen que la agrupación, a través de ellos, pueda ofrecer una forma de trabajar homogénea con unos elevados estándares de calidad, ampliando la posibilidad de compartir conocimientos y medios, y potenciando una coordinación en la atención conjunta a clientes comunes.

FILOSOFÍA DE TRABAJO

- Ejercicio tradicional y liberal de la profesión, con enfoque personalista y proximidad al cliente.
- El cliente se ve siempre atendido por un socio del despacho

CALIDAD EN SERVICIO

- El cliente tiene la posibilidad de realizar un seguimiento, las 24 horas del día y en tiempo real, de todas las actuaciones desarrolladas en cada uno de sus expedientes.
- Equipo profesional altamente cualificado, no sólo en las grandes capitales, sino en cualquier parte de la geografía nacional, que permite a nuestros clientes dar a sus filiales, delegaciones o sucursales un asesoramiento jurídico igual de eficaz y ágil que el que disponen en su oficina central.

- Comunicación directa con el despacho que está gestionando sus asuntos, sin intermediarios, ni terceros, ni necesidad de pasar por una sede central.

NUESTROS CLIENTES

- Grandes empresas que, como apoyo a sus propios departamentos jurídicos, necesitan saber que pueden contar con una cobertura jurídica nacional e internacional con despachos de primer nivel en cada una de las provincias españolas.
- Empresas locales con actividad comercial, estructura e intereses más allá del territorio provincial e incluso autonómico de cualquier sector de actividad.

VENTAJAS COMPETITIVAS DE LA EXTERNALIZACIÓN

- Estar al día de los constantes cambios, muchas veces en ámbitos locales, que se producen en el mundo del derecho
- Ahorro de tiempo por parte del personal directivo de una empresa que debe dedicar parte de su tiempo al control de las cuestiones jurídicas que se planteen.
- El apoyo de un asesoramiento jurídico externo resulta más ventajoso desde el punto de vista financiero.

ÁREAS DE ACTUACIÓN

- Administrativo
- Civil
- Fiscal
- Internacional
- Laboral
- Mercantil
- Nuevas Tecnologías
- Penal
- Procesal

CIFRAS HISPAJURIS

- Más de 500 profesionales
336 abogados
72 economistas
125 personas de soporte administrativo
- Más de 20 idiomas distintos.

RELACIÓN DE BUFETES MIEMBROS DE HISPAJURIS

ALBACETE

BUFETE MOLINA CABRERA, ABOGADOS & CONSULTORES DE EMPRESA FAMILIAR

Av. Isabel la Católica, 1-D; 4º-B
02005 ALBACETE
Tel: 967 21 43 09
Fax: 967 21 44 32
E-mail: bufetemolina@hispajuris.es

GONZALEZ & ABOGADOS ASOCIADOS, S.L.

Marqués de Molins, 13, 4º, dcha
02001 ALBACETE
Tel: 967 19 32 10
Fax: 967 24 09 73
E-mail: gonzalezabogados@hispajuris.es
Internet: www.gonzalezabogados.com

ALGECIRAS

BUFETE DIAZ Y ASOCIADOS, S.CV.

San Antonio, 1, 3ºB
11201 ALGECIRAS (CADIZ)
Tel: 956 63 16 87
Fax: 956 63 35 15
E-mail: bufetediaz@hispajuris.es
Internet: www.bufetediaz.com

ALICANTE

PÉREZ SEGURA ASOCIADOS, S.L.

Plaza san Cristóbal 2, 2º.
03002 ALICANTE
Tel: 96 521 99 55
Fax: 96 520 62 99
E-mail: perezsegura@hispajuris.es
Internet: www.perezsegura.com

ALMERÍA

INDAJURIS

Avda. Estación, 8. 8º - 2.
04005 ALMERÍA
Tel: 950. 28.11.61
Fax: 950.24.21.00
E-mail: indajuris@hispajuris.es
Internet: www.indajuris.com

ARANDA DE DUERO

J. MATEOS CUESTA & ASOCIADOS - DESPACHO DE ABOGADOS

Pza. Jardines de Don Diego, 6, 1º-E
09400 ARANDA DE DUERO (BURGOS)
Tel: 947 54 65 25
Fax: 947 54 61 25
E-mail: jmateos@hispajuris.es
Internet: www.jmateosabogados.com

BARCELONA

BASSOLS ADVOCATS & ECONOMISTES

Avda. Diagonal, 419 - 2º, 2ª
08008 BARCELONA
Tel: 93 415 99 00
Fax: 93 415 55 17 - 93 415 57 17
E-mail: bassols@hispajuris.es

BUFETE ESCURA, S.L.

Londres 43 Bajos
08029 BARCELONA
Tel: 93 494 01 31
Fax: 93 321 74 89
E-mail: escura@hispajuris.es
Internet: www.escura.com



BUFETE JURÍDICO FIGUERAS, S.L.

Borí Fontestá, 18, 4º, 1A.
08021 BARCELONA
Tel: 93 201 80 09
Fax: 93 200 17 62
E-mail: figueras@hispajuris.es
Internet: www.bufetefigueras.com

BILBAO

CALDERÓN & GARCÍA MORENO ABOGADOS, S.L.

C/ Juan de Ajuriaguerra nº 9, 2º.
48009 BILBAO
Tel: 944247188
Fax: 944242733
E-mail: calderonygarciamoreno@hispajuris.es
Internet: www.abogadoscgm.com

BURGOS

HERRERA CASTELLANOS GABINETE JURIDICO

Eduardo Martínez del Campo, 6 - Bajo
09003 BURGOS
Tel: 947 26 05 73
Fax: 947 25 76 20
E-mail: santiagoherrera@hispajuris.es

CÁCERES

CARMELO CASCÓN DESPACHO DE ABOGADOS

C/ León Leal, 1. 6º E
10002 Cáceres
Tel.: 927 62 70 74
Fax: 927 62 72 93
E-mail: carmelocascon@hispajuris.es
Contacto: D. Carmelo Cascón

CÁDIZ

BUFETE ESCALANTE ABOGADOS

Glorieta Santa Elena, 2. 5º C y D
11006 CÁDIZ
Tel: 956 20 12 19
Fax: 956 20 51 28
E-mail: bufeteescalante@hispajuris.es

CEUTA

BUFETE SANIN NARANJO

Beatriz de Silva, 7, Entlo.
11701 CEUTA
Tel: 956 51 31 31 - Fax: 956 51 29 81
E-mail: saninabogados@hispajuris.es

CIUDAD REAL

LOSA ABOGADOS

Pza. Cervantes, 4. 3º A
13001 CIUDAD REAL
Tel: 926 53 82 61 - Fax 926 21 22 73
E-mail: juanjoselosa@hispajuris.es

CÓRDOBA

BUFETE RICH & ASOCIADOS, S.L.

C/ San Fernando, 2.
14003 CÓRDOBA
Tel: 957485650 - Fax 957488858
E-mail: rich-asociados@hispajuris.es
Internet: www.rich-asociados.com

ELCHE

LUIS MARCO, POMARES Y ASOCIADOS, S.L.

Avda. País Valenciano nº19-11º
03201 ELCHE (Alicante)
Tel: 965 44 94 33 - Fax 966 674 100
E-mail: luismarco-pomares@hispajuris.es
Internet: www.luismarco-pomares.com

RELACIÓN DE BUFETES MIEMBROS DE HISPAJURIS

GIJÓN

VILIULFO DIAZ ABOGADOS Y ASESORES TRIBUTARIOS

Paseo de Begoña, 12 - Entres.
33201 GIJON (ASTURIAS)
Tel: 98 517 11 88
Fax: 98 517 11 92
E-mail: viliulfodiaz@hispaJuris.es
Internet: www.grupovd.com

GIRONA

ESTUDI LEGAL PEÑA HAITZ & INTERLEX, ADVOCATS ASSOCIATS

Pº. General Mendoza, nº 1, 7ª planta
17002 GIRONA
Tel: 972 41 31 61 - 972 41 26 71
Fax: 972 20 19 15
E-mail: estudilegal@hispaJuris.es
Internet: www.solucionsfamiliars.com

GGRANADA

HISPACOLEM SERVICIOS DE ASESORAMIENTO JURÍDICO Y EMPRESARIAL, S.L.

Trajano 8, esc. 1ª, 1º C
18002 GRANADA
Tel: 958 201 613 - 958 206 356
Fax: 958 201 697
E-mail: hispacolem@hispaJuris.es
Internet: www.hispacolem.com

LAS PALMAS

JIMÉNEZ BRITO ABOGADOS

Pza. España, 7. 3º H.
35007 Las Palmas de Gran Canaria.
Tel: 928 490533
Fax: 928 490533
E-mail: jimenez-brito@hispaJuris.es

LLEÓN

ÁLVAREZ-HIGUERA ABOGADOS, S.L.

Fuero, 13, 4º
24001 LEON
Tel: 987 20 05 01
Fax: 987 20 05 26
E-mail: alvarezhiguera@hispaJuris.es

LLEIDA

DESPATX MORAGUES, S.L.

Pza. Sant Joan, 18. 4º.
25007 LLEIDA
26002 Logroño (LA RIOJA)
Tel: 973 233733
Fax: 973 221551
E-mail: despatxmoragues@hispaJuris.es
Internet: www.despatxmoragues.com

LLOGROÑO

GIL-GIBERNAU ABOGADOS ASOCIADOS, S.L.

Vara del Rey, 15, 7º
26002 Logroño (LA RIOJA)
Tel: 941 259 900
Fax: 941 253 946
E-mail: gil-gibernau@hispaJuris.es
Internet: www.gil-gibernau.com

MMADRID

ABET & SAMPERE ASOCIADOS, S.L.

Villanueva, 35-37, 1º, 3
28001 MADRID
Tel: 91 781 92 00
Fax: 91 575 42 55
E-mail: absampere@hispaJuris.es
Internet: www.absampere.com



ALONSO Y ASOCIADOS - ABOGADOS

Príncipe de Vergara, 31, 4º-Izda.
28001 MADRID
Tel: 91 435 79 86 - 91 431 32 35 - 91 576 87 71
Fax: 91 576 54 63
E-mail: alonsoyasociados@hispajuris.es
Internet: www.alonsoyasociados.es

BUFETE ALEXANDER PITTS

Príncipe de Vergara, 10, 5º
28001 MADRID
Tel: 91 576 52 95
Fax: 91 577 55 42
E-mail: bapitts@hispajuris.es
Internet: www.bapitts.com

BUFETE INTERNACIONAL

Gurtubay, 6. 28001 MADRID
Tel: 91 435 05 55
Fax: 91 576 06 48
E-mail: bufeteinternacional@hispajuris.es
Internet: www.bufeteinternacional.com

MALAGA

ASELEX ASESORES LEGALES

Pirandello 6. Edificio Corona de Teatinos
Bloque 3, 2º Ofic. 4 y 5
29010 MALAGA
Tel: 952 27 27 11 - 952 27 19 12
Fax: 952 28 22 62
E-mail: aselex@hispajuris.es
Internet: www.aselex.es

MURCIA

GUILLÉN & ALBACETE ABOGADOS

Plaza de Santa Isabel nº12, 11ºB
30004 MURCIA
Tel: 968 21 38 88
Fax: 968 21 49 48
E-mail: guillenyalbacete@hispajuris.es
Internet: www.guillenyalbacete.com

PALMA DE MALLORCA

MON LEX ABOGADOS Y ASESORES TRIBUTARIOS

C/ Sindicato nº 67, 1º - 1ª
07002 Palma de Mallorca
Tel. 971.22 73 99
Fax 971.71 45 33
E-mail: mon-lex@hispajuris.es
Internet: www.mon-lex.com

SALAMANCA

MENDEZ MENDEZ ABOGADOS

C/ Villar y Macías 2, entreplanta
37002 SALAMANCA
Tel: 923 28 11 70
Fax: 923 28 17 87
E-mail: mendezabogados@hispajuris.es
Internet: www.mendezabogados.com

SANTANDER

PÉREZ DEL CAMINO ABOGADOS, S.L.

C/ Emilio Pino, 6. 7º. 39002
SANTANDER
Tel: 942. 22.62.06
Fax : 942.21.98.05
E-mail: perezdelcamino@hispajuris.es

RELACIÓN DE BUFETES MIEMBROS DE HISPAJURIS

SAN SEBASTIÁN

DE CARLOS & ASOCIADOS

Av. de la Libertad, 7-7ºD
20004 San Sebastián (GUIPUZCOA)
Tel: 943 42 13 37
Fax: 943 42 28 19
E-mail: decarlos@hispajuris.es
Internet: www.unigemsa.com

MUÑOZ-FRESCO ABOGADOS & ASESORES FISCALES

Gran Vía Marqués de Turia, 62-1º
46005 VALENCIA
Tel: 96 316 29 20
Fax: 96 374 47 03
E-mail: munozfresco@hispajuris.es
Internet: www.munozfresco.com

SANTA CRUZ DE TENERIFE

GOMEZ-TOLEDO ABOGADOS

Puerta Canseco, 79 - 3º
38003 SANTA CRUZ DE TENERIFE
Tel: 922 27 92 50 - 922 27 92 54
Fax: 922 24 68 64
E-mail: gomeztoledo@hispajuris.es

LMRV LUIS MIGUEL ROMERO VILLAFRANCA ABOGADOS

C/ Cirilo Amorós, nº 48
46004 VALENCIA
Tel: 96 351 78 36
Fax: 96 351 34 88
E-mail: lmromero@hispajuris.es

SEVILLA

BOLONIA ABOGADOS, SL.

Av. San Francisco Javier, 24, Planta 9ª,
mód. 12.
41018 Sevilla
Tel: 954 92 42 94 - 954 92 39 46
Fax: 954 92 22 81
E-mail: boloniaabogados@hispajuris.es
Internet: www.boloniaabogados.com
Contacto : Dª. Mª José Carracedo / D.
José Antonio Bosch

VALLADOLID

PALACIO PIMENTEL ABOGADOS

C/ Fray Luis de León, 22.
47002 VALLADOLID
Tel: 983 29 66 45
Fax: 983 39 64 03
E-mail: bufetejhernando@hispajuris.es

VALENCIA

PEDROS ABOGADOS

Colón, 20, 4º-8
46004 VALENCIA
Tel: 96 352 78 39
Fax: 96 352 85 18
E-mail: pedrosabogados@hispajuris.es

LITIS CONSULTING JURÍDICO

C/Galatea, 2. 5º A.
47004 VALLADOLID
Tel: 983 39 99 44
Fax: 983 21 04 79
E-mail: litis@hispajuris.es
Internet: www.litisjuridico.com



VIGO

SANTOS POUSA Y RODRÍGUEZ ABOGADOS S.L.

C/ Urzáiz, 40 – 3º

36201 VIGO

Tel: 986 22 60 10 / 11

Fax: 986 43 71 59

E-mail: santospousayrodriguez@hispajuris.es

Internet: www.santospousayrodriguez.com

PARIS

CABINET D'AVOCATS KAN-LACAS

5/7, Rue Georges Berger

75017 Paris

Tel: 0033.(0)1. 47 27 17 07

Fax: 0033.(0)1. 47 55 85 77

E-mail: kan-lacas.avocats@hispajuris.es

ZARAGOZA

ILEX ABOGADOS

Paseo de Sagasta, nº 17, pral. izda.

50008 ZARAGOZA

Tel: 976 22 33 80

Tel. 24 horas: 649 840 634

Fax: 976 21 79 39

E-mail: ilex@hispajuris.es

Internet: www.ilexabogados.com

HISPAJURIS EN EUROPA



Despachos miembros

BRUSELAS

KAISIN SZABO COLART & DE CASTRO

Advocaten - Avocats - Abogados

Avenue Louise/Louizalaan 391/8,

1050 Bruxelles/Brussel

Tel: 0032.2. 534 67 68

Fax: 0032.2. 640 01 79

E-mail: luisfdecastro@hispajuris.es



*Servicios jurídicos
en toda España*



Av. San Fco. Javier nº 24, Planta 9ª, mód. 12 41018 Sevilla
Tel. 954 924 294 • 954 923 946 Fax 954 922 281
boloniaabogados@hispanjuris.es www.boloniaabogados.com

patrocinado por: **BancoSabadell** 