Procedimiento nº.: PS/00517/2010
ASUNTO: Recurso de Reposición Nº RR/00314/2011

Examinado el recurso de reposición interpuesto por la entidad ***GESTORIA AGUSTI PLA I MARGARIT*** contra la resolución dictada por el Director de la Agencia Española de Protección de Datos en el procedimiento sancionador, PS/00517/2010, y en base a los siguientes,

HECHOS

PRIMERO: Con fecha 28 de febrero de 2011, se dictó resolución por el Director de la Agencia Española de Protección de Datos en el procedimiento sancionador, PS/00517/2010 , en virtud de la cual se imponía a la entidad ***GESTORIA AGUSTI PLA I MARGARIT*** una sanción de 4.000 €, por la vulneración de lo dispuesto en el artículo 9 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), infracción tipificada como grave el artículo 44.3.h de conformidad con lo establecido en el artículo 45.2,4 y 5 de la citada Ley Orgánica.

Dicha resolución, que fue notificada al recurrente en fecha 10/03/11, fue dictada previa la tramitación del correspondiente procedimiento sancionador, de conformidad con lo dispuesto en el artículo 127 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el reglamento de desarrollo de la LOPD.

SEGUNDO: Como hechos probados del citado procedimiento sancionador, PS/00517/2010, quedó constancia de los siguientes:

<<<<PRIMERO. Consta informe realizado por la policía local de Premiâ de Mar, relativo a una actuación policial en la calle Jacinto Verdaguer esquina con la calle la Plaça, referente al descubrimiento de diversa documentación de papel con datos personales.
(Folios 8-13)

SEGUNDO. Se remitió a esta Agencia la documentación localizada que se ha incorporado al expediente. La documentación se ha enviado en tres sobres rotulados como: como "1 ORIGINAL, "2 ORIGINAL PRUEBAS no datos personales" y "3 DOCUMENTOS DESTRUIDOS"

TERCERO. Los documentos que contienen datos personales los siguientes (Folios 35-159)

TIPO DE DOCUMENTO	*NÚMERO*
Permiso de residencia	*1 (dos copias)*

Permiso de conducir	*2*
Partes de accidente	*1 (y diversas copias)*
Proyecto de seguro	*1*
Escritura de sociedades	*1*
Pólizas de seguro automóvil	*4*
Pólizas de seguro hogar	*3*
Notas manuscritas	*3*
Justificante de correos	*6 (legible)*
Correo electrónico	*1*
Liquidaciones económicas	*3*
Movimientos bancarios	*1*

<u>CUARTO</u> Consta que la entidad Gestoría Pla Margarit se dedica a la correduría de seguros. Tiene su sede social en c/ Jacint Verdaquer nº 40 de Premiá de Mar (Folio 194)

<u>QUINTO</u> Consta que tienen inscritos en el Registro General de esta Agencia los siguientes ficheros:

"Correo Electrónico". Fichero de agenda y correos electrónicos para gestiones administrativas y contactos con clientes

"Contabilidad". Fichero para la gestión de la contabilidad general de la Empresa.

"Clientes". Fichero para gestiones administrativas y contacto con clientes

"Laboral". Fichero para la elaboración de nóminas y contratos de los trabajadores y relación de pago de nóminas

<u>SEXTO</u>. Que para el tratamiento de los ficheros anteriormente descritos en formato papel, se han establecido los siguientes mecanismos tal y como se establece en el documento de seguridad:

- Dispone de sistemas que aseguran la conservación y localización de documentos que almacenan datos de carácter personal.

- Cuando la documentación no se encuentra archivada porque se está trabajando con ella, la persona que se encuentra en su custodia impide que pueda acceder a la misma ninguna persona no autorizada.

- Los ficheros que contienen datos de nivel alto se encuentran en áreas en las que el acceso esté protegido con puertas de acceso que cuentan con sistemas de apertura mediante llave, estas se encuentran cerradas cuando no es preciso el acceso a los documentos.

- La generación de copias o la reproducción de documentos se realiza bajo el control del personal autorizado, por lo que no existe la posibilidad de que puedan darse copias no controladas de la documentación. (Folios 170-171)

<u>SEPTIMO.</u> Que dispone de destructora de papel, siendo destruidos por el propio personal de la gestoría los documentos en soporte papel que pudieran contener datos de carácter personal (Folio 195)

<u>OCTAVO.</u> Consta manifestación de la denunciada en el sentido que en fecha 20/10/09, la persona que realizaba la limpieza del despacho y el vaciado de papeleras, de manera involuntaria vació una de las bolsas de papel de pequeño tamaño. Por lo que esa documentación fue depositada en un contenedor de basura orgánica. Fue en ese momento cuando el personal de limpieza fue reprendido por la regidora de Medio Ambiente que solicitó la presencia de la policía local. (Folio 195) >>>>

<u>TERCERO</u>: ***GESTORIA AGUSTI PLA I MARGARIT*** (en los sucesivo el recurrente) ha presentado en fecha 11/04/11, en esta Agencia Española de Protección de Datos, recurso de

reposición fundamentándolo, básicamente, en
- *El material encontrado se refería a documentos antiguos.*
- *Parte del material no corresponde a ese despacho*
- *La empresa destruye la documentación y tiene ficheros debidamente registrados*
- *Los papeles fueron extraídos de un contenedor*

FUNDAMENTOS DE DERECHO

I

Es competente para resolver el presente recurso el Director de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (en lo sucesivo LRJPAC).

II

En relación con las manifestaciones efectuadas por ***GESTORIA AGUSTI PLA I MARGARIT,*** reiterándose básicamente, en las alegaciones ya presentadas a lo largo del procedimiento sancionador, debe señalarse que todas ellas ya fueron analizadas y desestimadas en los Fundamentos de Derecho del II al VIII ambos inclusive, de la Resolución recurrida, tal como se transcribe a continuación:

<<<<II

El art. 7 del Convenio Nº 108 del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, establece:

"Seguridad de los datos:
Se tomarán medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados."

El Art 17.1 de la Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, establece:

"Seguridad del tratamiento:
1. Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales. Dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse"

La ley Orgánica de Protección de Datos (en lo sucesivo LOPD), traspuso al ordenamiento interno el contenido de la Directiva 95/46. En el art. 32.1 de la citada Directiva se daba un plazo de tres años desde la adopción de la misma para la aprobación de las disposiciones legales que dieran cumplimiento a lo establecido en ella. Plazo que se extendía hasta los 12 años en relación a "el

tratamiento de los datos que ya se encuentran incluidos en ficheros manuales en la fecha de entrada en vigor de las disposiciones nacionales adoptadas en aplicación de la presente Directiva". En virtud de ello la disposición adicional primera de la LOPD establece un plazo de 12 años para la adecuación a la ley de los ficheros y tratamientos no automatizados, plazo que finalizó en octubre de 2007.

III

La LOPD en su artículo 1 dispone que "la presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar".

El artículo 2.1 de la misma ley orgánica establece: "1. La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento y a toda modalidad de uso posterior de estos datos por los sectores públicos y privados".

El artículo. 3 de la LOPD establece las definiciones de responsable de fichero o tratamiento, de encargado de tratamiento y de cesión de datos:

"d) Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento
…...
g) Encargado del tratamiento: La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento
……
I) Cesión o comunicación de datos: toda revelación de datos realizada a la persona distinta del interesado."

La vigente LOPD atribuye la condición de responsables de las infracciones a los responsables de los ficheros (art. 43), concepto que debe integrarse con la definición que de los mismos recoge el artículo 3.d), arriba citado, que incluye en el concepto de responsable tanto al que lo es del fichero como al del tratamiento de datos personales. En el presente caso, Gestoría Agustín Pla y Margarit es responsable de los ficheros y tratamientos, derivados de su actividad laboral, y en conformidad con las definiciones legales está sujeto al régimen de responsabilidad recogido en el Título VII de la LOPD.

IV

El artículo 9 de la LOPD, dispone:

"1. El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten la alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.
2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley."

Para poder delimitar cuáles sean los accesos que la Ley pretende evitar exigiendo las pertinentes medidas de seguridad es preciso acudir a las definiciones de "fichero" y "tratamiento" contenidas en la LOPD.

Sintetizando las previsiones legales puede afirmarse que:

a) Las operaciones y procedimientos técnicos automatizados o no, que permitan el acceso, –la comunicación o consulta- de datos personales, es un tratamiento sometido a las exigencias de la LOPD.

b) Los ficheros que contengan un conjunto organizado de datos de carácter personal así como el acceso a los mismos, cualquiera que sea la forma o modalidad en que se produzca están, también, sujetos a la LOPD.

c) La LOPD impone al responsable del fichero la adopción de medidas de seguridad, cuyo detalle se remite a normas reglamentarias, que eviten accesos no autorizados.

d) El mantenimiento de ficheros carentes de medidas de seguridad que permitan accesos o tratamientos no autorizados, cualquiera que sea la forma o modalidad de éstos, constituye una infracción tipificada como grave.

La documentación encontrada procedente de esa entidad entra en la consideración de documentación en soporte papel, contiene datos personales, debiéndosele aplicar las medidas de seguridad previstas reglamentaria a este tipo de ficheros y que han sido contempladas en el documento de seguridad de la denunciada.

Los hechos, que traen causa en este procedimiento, derivan de una denuncia motivada por que la persona que realizaba las tareas de limpieza en la entidad denunciada había arrojado, en un contenedor de basura orgánica, una bolsa de plástico que contenía documentación con datos de carácter personal y que se encontraba en las papeleras de la gestoría, junto a otro tipo de documentos.

El artículo 112 del RD 1720/07 de desarrollo de la LOPD establece lo siguiente:

"1.La generación de copias o la reproducción de los documentos únicamente podrá ser realizada bajo el control del personal autorizado en el documento de seguridad.
2. Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que evite el acceso a la información contenida en las mismas o a su recuperación posterior"

Se establece en este artículo las medidas que se tendrán que aplicar en los procesos de copia o reproducción de documentos. Haciendo mención especial a la necesidad de proceder a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o se recuperación posterior. Debe señalarse que el incumplimiento de este tipo de previsión implica un riesgo muy importante en la divulgación no deseada de documentos con batos personales,

Se impone en este articulo la obligación de adoptar medidas dirigidas a impedir el acceso o

manipulación de la información objeto de traslado, que incluye la atención a los protocolos que al respecto se deban aplicar cuando el traslado tenga como finalidad el desecho o destrucción de la documentación. Por lo tanto deberían de haberse adaptado, por parte de la entidad denunciada, las medidas suficientes que el acceso a la información contenida en los mismos, así como su posible recuperación posterior. Consecuencia que no se habían adaptado esas medidas, era que dicha documentación a destruir se encontraba intacta o rota en trozos lo suficientemente grandes, en las papeleras de la entidad denunciada, independientemente que mediara un descuido del personal de la limpieza que no introdujo la bolsa con la documentación en el contenedor de papel, si no en el de basuras orgánicas.

V

El hecho constatado en el presente procedimiento, relativo a la aparición de documentación procedente de la entidad denunciada en la vía publica y accesible a terceros supone una inobservancia del deber de adoptar las medidas de seguridad pertinentes por parte de la responsable del tratamiento

El artículo 44.3 h) califica como infracción grave: "Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen". De acuerdo con los fundamentos anteriores, se deduce que por parte de la entidad denunciada se ha producido una vulneración de la de seguridad de los datos, que ha tenido como consecuencia que los datos personales, pudieran ser vistos por un tercero, infracción que procede calificarla en el grado señalado.

La exigencia de la "culpabilidad" deriva de lo que señala el articulo 130 de la Ley 30/92, de 26 de noviembre, de Régimen Jurídico de las Administraciones Publicas y del Procedimiento Administrativo Común – LRJPAC- cuando dice que: "Sólo podrán ser sancionadas por hechos constitutivos de infracción administrativa las personas físicas y jurídicas que resulten responsables de los mismos aun a título de simple inobservancia".

Si bien en materia sancionadora rige el principio de culpabilidad, la expresión "simple inobservancia", del art. 130.1 de la Ley 30/92, permite la sanción por inobservancia del deber de cuidado. Tal es la interpretación que ha establecido la Audiencia Nacional en la sentencia de 6/02/08. Existe una obligación de resultado, que no se ha cumplido, pues documentación con datos de carácter personal procedente de la entidad denunciada se encontró si destruir en una bolsa de basura, de lo que se desprende una falta de negligencia del responsable del tratamiento, obligado a implementar las medidas de seguridad. La necesidad de especial diligencia en la custodia de la documentación por parte del responsable y encargado del tratamiento ha sido puesta de relieve por la Audiencia Nacional, en diversas sentencias, en particular en la sentencia de 25/06/09, Rec. 237/2008, que manifiesta: "Es doctrina reiterada en esta Sala, SSAN, sec. 1ª, de 25/1/06 (re. 227/2004), 28/06/06 (Re. 290/2004), que "No basta con la aplicación formal de las medidas de seguridad, pues resulta exigible que aquellas se instauren y pongan en práctica de manera efectiva…Se impone, en consecuencia, una obligación de resultado, consistente en que se adopten las medidas necesarias para evitar que los datos se pierdan, extravíen o acaben en manos de terceros. En definitiva la recurrente es, por disposición legal, una deudora de seguridad en materia de datos y puesto que es una deudora de seguridad en materia de datos es insuficiente, según se desprende la doctrina de la Sala que se acaba de exponer, con acreditar que se adoptaron una serie de medidas, pues dicha entidad también es responsable de que las mismas se cumplan y ejecuten con rigor"

La presencia de un descuido de la persona que realizaba las tareas de limpieza no puede

exonerar la responsabilidad de la denunciada, obligada a implementar las medidas de seguridad adecuadas. En base a la interpretación dado por la Audiencia Nacional, en la recurso 559/2007, que desestimaba el recurso de una entidad basado en la existencia de responsabilidad de unos de sus empleados: "Es cierto que dicha entidad bancaria acredita el cumplimiento de las medidas de seguridad, tanto en sus sucursales, como respecto de su personal, en los términos exigidos por la LOPD, y también es cierto que fue un empleado de dicha entidad el que provocó los hechos ahora sancionados. Más esta Sala ha declarado con reiteración, en las sentencias reseñadas en el fundamento jurídico anterior e igualmente en la SAN de 14-2-2007 (Rec. 229/2005 , entre otras) que no basta con la aprobación formal de las medidas de seguridad, pues resulta exigible que aquéllas se instauren y pongan en práctica de manera efectiva. Así, de nada sirve que se aprueben unas instrucciones detalladas sobre el modo de proceder para la recogida y destrucción de documentos que contengan datos personales si luego no se exige a los empleados del banco la observancia de aquellas instrucciones. Por lo que necesariamente te ha de concluir que …. debió adoptar las medidas necesarias para impedir cualquier recuperación por terceros no autorizados de la información reservada a la que tuvo acceso la empresa de limpieza, y al no efectuarlo así, no observó la diligencia necesaria, pues de otro modo no se explica que un importante volumen de documentos de uso interno de la entidad (a la denuncia se acompañaba una gran caja), en muchos de los cuales figuraban datos personales, fueran a parar a manos de tal concesionaria de la recogida de basura."

VI

El artículo 10 de la LOPD establece que: "El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo".

El deber de confidencialidad obliga no sólo al responsable del fichero sino a todo aquel que intervenga en cualquier fase del tratamiento. Dado el contenido del precepto, ha de entenderse que el mismo tiene como finalidad evitar que por parte de quienes están en contacto con los datos personales almacenados en ficheros se realicen filtraciones de los datos no consentidas por los titulares de los mismos. Así el Tribunal Superior de Justicia de Madrid ha declarado en su Sentencia de 19 de julio de 2001: "El deber de guardar secreto del artículo 10 queda definido por el carácter personal del dato integrado en el fichero, de cuyo secreto sólo tiene facultad de disposición el sujeto afectado, pues no en vano el derecho a la intimidad es un derecho individual y no colectivo. Por ello es igualmente ilícita la comunicación a cualquier tercero, con independencia de la relación que mantenga con él la persona a que se refiera la información (...)".

En este sentido, la sentencia de la Audiencia Nacional de fecha 18 de enero de 2002, recoge en su Fundamento de Derecho Segundo, y tercer párrafo: "El deber de secreto profesional que incumbe a los responsables de ficheros automatizados, recogido en el artículo 10 de la Ley Orgánica 15/1999, comporta que el responsable –en este caso, la entidad bancaria recurrente- de los datos almacenados –en este caso, los asociados a la denunciante- no puede revelar ni dar a conocer su contenido teniendo el "deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero automatizado o, en su caso, con el responsable del mismo" (artículo 10 citado). Este deber es una exigencia elemental y anterior al propio reconocimiento del derecho fundamental a la libertad informática a que se refiere la STC 292/2000, y por lo que ahora interesa, comporta que los datos tratados automatizadamente no pueden ser conocidos por ninguna persona o entidad, pues en eso consiste precisamente el secreto.

Este deber de sigilo resulta esencial en las sociedades actuales cada vez más complejas, en las que los avances de la técnica sitúan a la persona en zonas de riesgo para la protección de derechos fundamentales, como la intimidad o el derecho a la protección de los datos que recoge el artículo 18.4 de la CE. En efecto, este precepto contiene un "instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los derechos de los ciudadanos que, además, es en sí mismo un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos" (STC 292/2000). Este derecho fundamental a la protección de los datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino" (STC 292/2000) que impida que se produzcan situaciones atentatorias con la dignidad de la persona, "es decir, el poder de resguardar su vida privada de una publicidad no querida"

En el caso que nos ocupa, la entidad denunciada es responsable de la custodia de la documentación relativa a sus clientes, que ha sido recuperada por el denunciante, existiendo pues, una omisión del deber de secreto, produciéndose una ausencia de confidencialidad, por lo que se considera que se ha cometido una infracción del transcrito artículo 10 de la LOPD.

VII

El artículo 44.3.g) de la LOPD, califica como infracción grave:

"La vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo"

De acuerdo con los fundamentos anteriores, se deduce que por parte de la entidad denunciada se ha producido una vulneración del deber de secreto y de seguridad de los datos, infracciones que procede calificarlas como graves. Sin que pueda exonerarse su responsabilidad tal como se ha demostrado en este procedimiento, por lo que procede su imputación, elemento necesario en el derecho administrativo sancionador tal como establece la STS de 27/5/99: "Para la imposición de una sanción y las consecuencias derivadas del ilícito administrativo, no basta que la infracción esté tipificada y sancionada…sino que es necesario que se aprecie en el sujeto infractor el elemento o categoría denominado culpabilidad. La culpabilidad es el reproche que se hace a una persona, porque ésta debió haber actuado de modo distinto de cómo lo hizo".

VIII

El hecho constatado de la difusión de datos personales fuera del ámbito de la entidad denunciada establece la base de facto para fundamentar la imputación de las infracciones de los artículos 9 y 10 de la LOPD.

No obstante, nos encontramos ante un supuesto en el que un mismo hecho deriva en dos infracciones, dándose la circunstancia que la comisión de una implica necesariamente la comisión de la otra. Esto es, si un documento interno que contiene información sobre datos personales sale del ámbito de la entidad responsable de su confidencialidad, se está produciendo un incumplimiento de las medidas de seguridad exigidas a dicho responsable que, a su vez, deriva en una vulneración del deber de secreto.

Por lo tanto, aplicando el artículo 4.4 del Real Decreto 1398/1993, de 4 de agosto, por el que se aprueba el Reglamento del procedimiento para el ejercicio de la potestad sancionadora que señala que "en defecto de regulación específica establecida en la norma correspondiente, cuando de la comisión de una infracción derive necesariamente la comisión de otra u otras, se deberá imponer únicamente la sanción correspondiente a la infracción más grave cometida", procede subsumir ambas infracciones en una. Dado que, en este caso, se ha producido una vulneración de las medidas de seguridad, calificada como grave por el artículo 44.3.h) de la LOPD y también un incumplimiento del deber de guardar secreto, calificado como grave en el artículo 44.3.g) de la misma norma, procede imputar únicamente la infracción del artículo 9 de la LOPD.>>>>

III

La ley 2/2011, de 4 de marzo, de Economía Sostenible, disposición final quincuagésima sexta, ha venido a modificar el art. 45 de la LOPD que ha quedado redactado de la siguiente forma. Dichas modificaciones se han aplicado al presente caso dado su carácter de norma más favorable:

"1*. Las infracciones leves serán sancionadas con multa de 900 a 40.000 euros.*

2. Las infracciones graves serán sancionadas con multa de 40.001 a 300.000 euros.

3. Las infracciones muy graves serán sancionadas con multa de 300.001 a 600.000 euros.

4. La cuantía de las sanciones se graduará atendiendo a los siguientes criterios:

a) El carácter continuado de la infracción.
b) El volumen de los tratamientos efectuados.
c) La vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal.
d) El volumen de negocio o actividad del infractor.
e) Los beneficios obtenidos como consecuencia de la comisión de la infracción.
f) El grado de intencionalidad.
g) La reincidencia por comisión de infracciones de la misma naturaleza.
h) La naturaleza de los perjuicios causados a las personas interesadas o a terceras personas.
i) La acreditación de que con anterioridad a los hechos constitutivos de infracción la entidad imputada tenía implantados procedimientos adecuados de actuación en la recogida y tratamiento de los datos de carácter personal, siendo la infracción consecuencia de una anomalía en el funcionamiento de dichos procedimientos no debida a una falta de diligencia exigible al infractor.
j) Cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.

5. El órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate, en los siguientes supuestos:

a) Cuando se aprecie una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho como consecuencia de la concurrencia significativa de varios de los criterios enunciados en el apartado 4 de este artículo.
b) Cuando la entidad infractora haya regularizado la situación irregular de forma diligente.
c) Cuando pueda apreciarse que la conducta del afectado ha podido inducir a la comisión de la infracción.
d) Cuando el infractor haya reconocido espontáneamente su culpabilidad.
e) Cuando se haya producido un proceso de fusión por absorción y la infracción fuese anterior a

dicho proceso, no siendo imputable a la entidad absorbente".

La citada disposición adicional ha venido a añadir un nuevo apartado 6 al artículo 45, cuyo texto es el siguiente:

"6. Excepcionalmente el órgano sancionador podrá, previa audiencia de los interesados y atendida la naturaleza de los hechos y la concurrencia significativa de los criterios establecidos en el apartado anterior, no acordar la apertura del procedimiento sancionador y, en su lugar, apercibir al sujeto responsable a fin de que, en el plazo que el órgano sancionador determine, acredite la adopción de las medidas correctoras que en cada caso resultasen pertinentes, siempre que concurran los siguientes presupuestos:

a) Que los hechos fuesen constitutivos de infracción leve o grave conforme a lo dispuesto en esta Ley.
b) Que el infractor no hubiese sido sancionado o apercibido con anterioridad.
Si el apercibimiento no fuera atendido en el plazo que el órgano sancionador hubiera determinado procederá la apertura del correspondiente procedimiento sancionador por dicho incumplimiento."

En la nueva redacción dada en la citada Ley 2/2011 al artículo 44 de la LOPD, se tipifica como infracción grave, en el apartado 44.3.h "*mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal, sin las debidas condiciones de seguridad que vía reglamentaria se determinen"*, en consecuencia no se ha producido un cambio en la tipificación de la infracción cometida por la entidad denunciada en base los hechos probados en este procedimiento y su calificación jurídica.

Ahora bien, del principio constitucional, establecido en el artículo 9.3 que garantiza la irretroactividad de las disposiciones sancionadoras no favorables, se deduce, como principio que ha sido recogido por la legislación positiva, la retroactividad de las disposiciones posteriores favorables al infractor, (aplicable a aquellos procedimientos que no sean firmes) , en particular en la Ley 30/1992, de 26 de noviembre de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común –que, al decir de su Exposición de Motivos (punto 17) recoge "*los principios básicos a que debe someterse el ejercicio de la potestad sancionadora de la Administración y los correspondientes derechos que de tales principios se derivan para los ciudadanos extraídos del Texto Constitucional y de la ya consolidada jurisprudencia sobre la materia*"- sanciona el principio de aplicación retroactiva de la norma más favorable estableciendo en el artículo 127.2 que "*las disposiciones sancionadoras producirán efecto retroactivo en cuanto favorezcan al presunto infractor*".

En el presente supuesto, de la alegaciones presentadas por la entidad denunciada y los hechos probados en el expediente, se deduce que se cumplen los requisitos recogidos en los apartados a) y b) del citado apartado 6, que motivan suficientemente la estimación del presente recurso interpuesto contra la resolución de fecha 28/2/11, anulando sanción impuesta a la entidad denunciada, sin perjuicio de la derivación en un procedimiento de apercibimiento en base a la aplicación de la legislación más favorable. Debiéndose tenerse en cuenta:
- Que es un hecho puntual.
- Se trata de una empresa con pequeño volumen de tratamientos
- Inexistencia de beneficios
- No ha existido intencionalidad, se trata de un error
- Que han sido pocos los documentos con datos de carácter personal depositados en la basura - Que hay implementados una serie de mecanismos para el tratamiento de los ficheros y la destrucción de los documentos en formato papel, establecidos en el documento de seguridad:
- Dispone de sistemas que aseguran la conservación y localización de documentos que almacenan

datos de carácter personal.
- Que dispone de destructora de papel, siendo destruidos por el propio personal de la gestoría los documentos en soporte papel que pudieran contener datos de carácter personal

El Director de la Agencia Española de Protección de Datos **RESUELVE:**

PRIMERO: ESTIMAR el recurso de reposición interpuesto por ***GESTORIA AGUSTI PLA I MARGARIT*** contra la Resolución de esta Agencia Española de Protección de Datos dictada con fecha 28 de febrero de 2011, en el procedimiento sancionador PS/00517/2010, indicando al sancionado que queda sin efecto la obligación de abonar la multa impuesta en la Resolución recurrida.

SEGUNDO: APERCIBIR A ***GESTORIA AGUSTI PLA I MARGARIT*** con arreglo a lo dispuesto en el artículo 45.6 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, con relación a la denuncia por infracción del artículo 9 de la LOPD, tipificada como grave en el artículo 44.3.h) de la citada Ley Orgánica y de conformidad con lo establecido en los artículos 36 y 37.a), f) y n) de la LOPD, que atribuye la competencia al Director de la Agencia Española de Protección de Datos.

TERCERO: Teniéndose en cuenta la naturaleza de la infracción no se interesan actuaciones concretas de necesaria adaptación por esta Agencia, no obstante se **REQUiERE** A ***GESTORIA AGUSTI PLA I MARGARIT*** para que comunique las medidas que decidan adoptar y que supongan mayores garantías para que en el futuro no vuelva a producirse una infracción por inobservancia del artículo 9 de la LOPD

CUARTO: **NOTIFICAR I**a presente resolución a la entidad ***GESTORIA AGUSTI PLA I MARGARIT.***

De conformidad con lo establecido en el apartado 2 del artículo 37 de la LOPD, en la redacción dada por el artículo 82 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, la presente Resolución se hará pública, una vez haya sido notificada a los interesados. La publicación se realizará conforme a lo previsto en la Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones y con arreglo a lo dispuesto en el artículo 116 del Real Decreto 1720/2007, de 21 diciembre, por el que se aprueba el reglamento de desarrollo de la LOPD.

Contra esta resolución, que pone fin a la vía administrativa, se podrá interponer en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto según lo previsto en el artículo 46.1 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta del referido texto legal.

Madrid, 30 de mayo de 2011

EL DIRECTOR DE LA AGENCIA ESPAÑOLA
DE PROTECCIÓN DE DATOS

Fdo.: Artemi Rallo Lombarte