Procedimiento Nº: A/00269/2016

RESOLUCIÓN: R/02748/2016

En el procedimiento A/00269/2016, instruido por la Agencia Española de Protección de Datos a la entidad ***RSM CORREDURÍA DE SEGUROS, S.A..***, vista la denuncia presentada por D. ***B.B.B.*** y en virtud de los siguientes,

ANTECEDENTES

PRIMERO: Con fechas 24 y 30/05/2016, tuvieron entrada en esta Agencia sendos escritos de D. ***B.B.B.*** (en lo sucesivo el denunciante), en los que formula denuncia contra la entidad RSM Correduría de Seguros, S.A. por la publicación de sus datos personales en el sitio web de la entidad, www.rsmseguros.es, concretamente, el relativo a su DNI, que aparece asociado a la mercantil en la que trabaja. Añade que dicha publicación se ha realizado sin su consentimiento.

De la documentación aportada se desprende que, al consultar en Google por el número de su DNI se obtiene un resultado vinculado al sitio web www.rsmseguros.es, apareciendo en la página de resultados un resumen (snippet) que incluye cuatro números de DNI, entre ellos el del afectado, junto al nombre de una mercantil.

SEGUNDO: Con fecha 27/05/2016, tras recibirse el primer escrito de denuncia, por la Subdirección General de Inspección de Datos se realizó una búsqueda en Google con el número de DNI del denunciante como criterio, obteniéndose en la página de resultados un enlace a la dirección web (url) " ***A.A.A.***", junto a un resumen que incluía el texto: "*No hay disponible una descripción de este resultado debido al archivo robots.txt de este sitio. Más información*". Al seleccionar el enlace se accedía a una página sin datos personales. Se verificó, asimismo, que en el fichero www.rmseguros.es/robots.txt figuraba una instrucción a todos los robots (*) para que no indexaran ningún contenido del sitio web (/). Se realizó la misma búsqueda en el buscador Bing, no obteniéndose resultados vinculados al dominio *rmseguros.es.*

TERCERO: Con fecha 11/07/2016, la Directora de la Agencia Española de Protección de Datos, por virtud de lo dispuesto en el artículo 45.6 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), acordó someter a la entidad RSM Correduría de Seguros, S.A. a trámite de audiencia previa al apercibimiento por la presunta infracción del artículo 9 de dicha norma, en relación con los artículos 91 y 93 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, tipificada como grave en el artículo 44.3.h) de la citada Ley Orgánica.

CUARTO: Iniciado el procedimiento, el denunciante presentó escrito en el que manifiesta que Google eliminó sus datos personales a petición suya y reitera que no ha tenido concertada ninguna póliza de seguros con la mercantil RSM Correduría de Seguros, S.A., a pesar de que dicha entidad, en respuesta al derecho de acceso

ejercitado por el mismo, le comunicó que dispone de sus datos personales por haber tenido contratada alguna póliza con su mediación.

Aporta copia de las comunicaciones dirigidas a Google solicitando la eliminación del enlace objeto de la denuncia y la respuesta de esta entidad indicando que su solicitud será procesada.

QUINTO: RSM Correduría de Seguros, S.A., por su parte, presentó escrito de alegaciones en el que solicita el archivo del expediente en base a las consideraciones siguientes:

. En el momento en que se formula la denuncia, los datos personales del denunciante contenidos en su web habían sido desindexados.

. Insiste en que el denunciante fue cliente de la entidad, pero señala que el dato relativo al DNI del mismo estaba vinculado al sitio web de RSM Correduría de Seguros, S.A. en su condición de trabajador de una empresa concesionaria de automoción que actúa como colaborador externo de la correduría. En base a esta relación, el denunciante tiene acceso limitado a la aplicación informática de la entidad y utiliza su número de DN como id de usuario.

. Una vez RSM Correduría de Seguros, S.A. conoció que el DNI aparecía en los resultados de búsqueda, en fecha 11/05/2016 se creó un fichero robots.txt para evitar la indexación de los contenidos de la aplicación informática, incluyendo la utilizada por los colaboradores externos.

HECHOS PROBADOS

1. La entidad RSM Correduría de Seguros, S.A. es titular de la web www.rsmseguros.es.

2. Utilizando el buscador de internet Google, con el número de DNI del denunciante como criterio de búsqueda, se obtenía en la página de resultados un enlace al sitio web www.rsmseguros.es que posibilitaba el acceso al DNI del denunciante asociado a la mercantil en la que trabaja.

3. Con fecha 27/05/2016, por la Subdirección General de Inspección de Datos se realizó una búsqueda en Google con el número de DNI del denunciante como criterio, obteniéndose en la página de resultados un enlace a la dirección web (url) " ***A.A.A.***", junto a un resumen que incluía el texto: "*No hay disponible una descripción de este resultado debido al archivo robots.txt de este sitio. Más información*". Al seleccionar el enlace se accedía a una página sin datos personales. Se verificó, asimismo, que en el fichero www.rmseguros.es/robots.txt figuraba una instrucción a todos los robots (*) para que no indexaran ningún contenido del sitio web (*/*). Se realizó la misma búsqueda en el buscador Bing, no obteniéndose resultados vinculados al dominio *rmseguros.es.*

FUNDAMENTOS DE DERECHO

I

Es competente para resolver este procedimiento la Directora de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto en el artículo 37. g) en relación con el artículo 36 de la LOPD.

II

El Titulo VII sobre *Infracciones y sanciones*, en el artículo 43, de la LOPD establece:

"1. Los responsables de los ficheros y los encargados de los tratamientos estarán sujetos al régimen sancionador establecido en la presente Ley."

El artículo. 3 de la LOPD establece la definición de responsable de fichero o tratamiento y del encargado del tratamiento:

"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".

III

El artículo 18.4 de la Constitución Española establece en que: *"la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*", consagrándose así el derecho a la protección de datos como un derecho autónomo, incluso del propio derecho a la intimidad, tal y como ha indicado la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre.

El artículo 1 de la LOPD dispone: *"La presente Ley Orgánica 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 y familiar".*

En cuanto al ámbito de aplicación de la citada norma, el artículo 2.1 de la misma señala que *"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 público y privado"*; definiéndose el concepto de dato de carácter personal en el artículo 3.a) de la citada LOPD como *"Cualquier información concerniente a personas físicas identificadas o identificables"*.

En este mismo sentido se pronuncia el artículo 2.a) de la Directiva 95/46/CE, del Parlamento y del Consejo, de 24/10/1995, 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 (en lo sucesivo la Directiva), según el cual se entiende por dato personal *"toda información sobre una persona física identificada o identificable; se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente,*

en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social".

En el presente caso, ha quedado acreditado que el fichero accedido, atendiendo a su contenido (DNI del denunciante y entidad en la que presta servicios como trabajador), se encuentra incluido dentro del ámbito de aplicación establecido en la LOPD y sus normas de desarrollo.

IV

Se imputa a la entidad RSM Correduría de Seguros, S.A. el incumplimiento del principio de seguridad de los datos personales que constan en sus ficheros.

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 LOPD, traspuso al ordenamiento interno el contenido de la Directiva 95/46. En el artículo 9 de la citada LOPD se dispone lo siguiente:

"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".

El trascrito artículo 9 de la LOPD establece el *"principio de seguridad de los datos"* imponiendo la obligación de adoptar las medidas de índole técnica y organizativa que garanticen dicha seguridad, añadiendo que tales medidas tienen como finalidad evitar, entre otros aspectos, el *"acceso no autorizado"* por parte de terceros.

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.

En lo que respecta al concepto de "*fichero*" el artículo 3.b) de la LOPD lo define como *"todo conjunto organizado de datos de carácter personal",* con independencia de la modalidad de acceso al mismo.

Por su parte el artículo 3.c) de la citada Ley Orgánica considera tratamiento de datos cualquier operación o procedimiento técnico que permita, en lo que se refiere al objeto del presente procedimiento, la *"comunicación"* o *"consulta"* de los datos personales tanto si las operaciones o procedimientos de acceso a los datos son automatizados o no.

Para completar el sistema de protección en lo que a la seguridad afecta, el artículo 44.3.h) de la LOPD tipifica como infracción grave el mantener los ficheros *"...que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen".*

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.

Las medidas de seguridad se clasifican en atención a la naturaleza de la información tratada, esto es, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la misma. Dichas medidas, en el caso que nos

ocupa, deben salvaguardar la confidencialidad y seguridad de los datos de carácter personal contenidos en los ficheros de la entidad RSM Correduría de Seguros, S.A., declarado en el Registro General de Protección de Datos con nivel de seguridad medio.

Las medidas de seguridad de nivel básico están reguladas en los artículos 89 a 94, las de nivel medio se regulan en los artículos 95 a 100 y las medidas de seguridad de nivel alto se regulan en los artículos 101 a 104, del Reglamento de desarrollo de la LOPD.

Los artículos 91 y 93 del citado Reglamento, aplicable a todos los ficheros y tratamientos automatizados, establecen:

"Artículo 91. Control de acceso.

1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.
2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.
3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.
4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.
5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio".

Este artículo desarrolla las previsiones que deberá establecer el responsable del fichero para garantizar que los usuarios con accesos a datos personales o recursos, por haber sido previamente autorizados, sólo puedan acceder a tales datos y recursos. Para ello es necesario que se implanten mecanismos de control para evitar que un usuario pueda acceder a datos o funcionalidades que no se correspondan con el tipo de acceso autorizado para el mismo, en función del perfil de usuario asignado.

"Artículo 93. Identificación y autenticación.

1. El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.
2. El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.
3. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.
4. El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible".

El artículo 5.2.b) del citado Reglamento define la "autenticación" como el procedimiento de comprobación de la identidad de un usuario; y el mismo artículo, letra

h), se refiere a la "identificación" como el procedimiento de reconocimiento de la identidad de un usuario. Corresponde al responsable del fichero o tratamiento comprobar la existencia de la autorización exigida en el citado artículo 91, con un proceso de verificación de la identidad de la persona (autenticación) implantando un mecanismo que permita acceder a datos o recursos en función de la identificación ya autenticada. Cada identidad personal deberá estar asociada con un perfil de seguridad, roles y permisos concedidos por el responsable del fichero o tratamiento.

En definitiva, según las normas expuestas, RSM Correduría de Seguros, S.A. está obligada a adoptar las medidas técnicas y organizativas para garantizar la seguridad de los datos e impedir el acceso no autorizado por parte de terceros a los mismos. Sin embargo, ha quedado acreditado que la citada entidad incumplió esta obligación, al haberse constatado que utilizando un buscador de internet, con el DNI como criterio de búsqueda, se obtenía un enlace a la web www.rsmseguros.es que permitía el acceso sin restricción alguna a ese dato personal del denunciante asociado a la mercantil en la que trabaja como empleado.

Esta irregularidad, es decir, la posibilidad de que cualquier tercero pudiera acceder a la información indicada, resulta de un fallo de seguridad que ha sido reconocido por la propia entidad imputada, al no haber establecido mecanismos que impidieran la indexación de contenidos por buscadores de internet.

Así, los datos personales del denunciante resultaron accesibles por parte de terceros a través de la web de RSM Correduría de Seguros, S.A., siendo ello consecuencia de una insuficiente o ineficaz implementación de las medidas de seguridad. Dado que ha existido vulneración del *"principio de seguridad de los datos"*, se considera que RSM Correduría de Seguros, S.A. ha incurrido en la infracción tipificada como grave en el artículo 44.3.h) de la LOPD, que considera como tal *"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"*.

V

En esta materia se impone una obligación de resultado, que conlleva la exigencia de que las medidas implantadas deben impedir, de forma efectiva, el acceso a la información por parte de terceros. Esta necesidad de especial diligencia en la custodia de la información por el responsable ha sido puesta de relieve por la Audiencia Nacional, en su Sentencia de 11/12/08 (recurso 36/08), fundamento cuarto: *"Como ha dicho esta Sala en múltiples sentencias…se impone, en consecuencia, una obligación de resultado, consistente en que se adoptan las medidas necesarias para evitar que los datos se pierdan, extravíen o acaben en manos de terceros…la recurrente es, por disposición legal una deudora de seguridad en materia de datos, y por tanto debe dar una explicación adecuada y razonable de cómo los datos han ido a parar a un lugar en el que son susceptibles de recuperación por parte de terceros, siendo insuficiente con acreditar que adopta una serie de medidas, pues es también responsable de que las mismas se cumplan y se ejecuten con rigor".*

El principio de culpabilidad es exigido en el procedimiento sancionador y así la STC 246/1991 considera inadmisible en el ámbito del Derecho administrativo sancionador una responsabilidad sin culpa. Pero el principio de culpa no implica que

sólo pueda sancionarse una actuación intencionada y a este respecto el artículo 130.1 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, dispone *"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."*

El Tribunal Supremo (STS 16 de abril de 1991 y STS 22 de abril de 1991) considera que del elemento culpabilista se desprende *"que la acción u omisión, calificada de infracción sancionable administrativamente, ha de ser, en todo caso, imputable a su autor, por dolo o imprudencia, negligencia o ignorancia inexcusable."* El mismo Tribunal razona que *"no basta...para la exculpación frente a un comportamiento típicamente antijurídico la invocación de la ausencia de culpa" sino que es preciso "que se ha empleado la diligencia que era exigible por quien aduce su inexistencia."* (STS 23 de enero de 1998).

A mayor abundamiento, la Audiencia Nacional en materia de protección de datos de carácter personal, ha declarado que *"basta la simple negligencia o incumplimiento de los deberes que la Ley impone a las personas responsables de ficheros o del tratamiento de datos de extremar la diligencia..."*(SAN 29de junio de 2001).

En definitiva, ha de señalarse que es la entidad RSM Correduría de Seguros, S.A. la obligada garantizar la seguridad de los datos, asegurando la efectividad de las medidas adoptadas.

VI

Por otra parte, se tuvo en cuenta que RSM Correduría de Seguros, S.A. no ha sido sancionada o apercibida con anterioridad por esta Agencia. En consecuencia, de conformidad con lo establecido en el artículo 45.6 de la LOPD, se acordó someter a la citada entidad a trámite de audiencia previa al apercibimiento, en relación con la denuncia por infracción del artículo 9 de la LOPD.

El citado apartado 6 del artículo 45 de la LOPD establece lo siguiente:

"*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 el presente supuesto se cumplen los requisitos recogidos en los apartados a)

y b) del citado artículo 45.6 de la LOPD. Junto a ello, se constata una cualificada disminución de la culpabilidad de la imputada teniendo en cuenta el volumen de datos personales afectados por la incidencia y su naturaleza, la ausencia de perjuicios distintos a los que derivan de la misma y ausencia de beneficios, así como la inmediata respuesta de RSM Correduría de Seguros, S.A. para subsanar la incidencia.

Todo ello, justifica que la AEPD no acordara la apertura de un procedimiento sancionador y que optase por aplicar el artículo 45.6 de la LOPD.

Ahora bien, es obligado hacer mención a la Sentencia de la Audiencia Nacional de 29/11/2013, (Rec. 455/2011), Fundamento de Derecho Sexto, que sobre el apercibimiento regulado en el artículo 45.6 de la LOPD y a propósito de su naturaleza jurídica advierte que "*no constituye una sanción"* y que se trata de "*medidas correctoras de cesación de la actividad constitutiva de la infracción"* que *sustituyen* a la sanción. La Sentencia entiende que el artículo 45.6 de la LOPD confiere a la AEPD una "*potestad"* diferente de la sancionadora cuyo ejercicio se condiciona a la concurrencia de las especiales circunstancias descritas en el precepto.

En congruencia con la naturaleza atribuida al apercibimiento como una alternativa a la sanción cuando, atendidas las circunstancias del caso, el sujeto de la infracción no es merecedor de aquella, y considerando que el objeto del apercibimiento es la imposición de medidas correctoras, la SAN citada concluye que cuando éstas ya hubieran sido adoptadas, lo procedente en Derecho es acordar el archivo de las actuaciones.

Como se ha señalado en el Hecho Probado Tercero, en el asunto analizado, consta que se ha impedido el acceso por parte de terceros a los datos personales contenidos en la web www.rsmseguros.es. En concreto, por la Subdirección General de Inspección de Datos se comprobó el enlace a dicha web obtenido utilizando buscadores de internet incluía el texto: "*No hay disponible una descripción de este resultado debido al archivo robots.txt de este sitio. Más información*" y no ofrecía ningún dato personal.

Se verificó, asimismo, que en el fichero www.rmseguros.es/robots.txt figuraba una instrucción a todos los robots (*) para que no indexaran ningún contenido del sitio web (/).

Por tanto, a la vista del pronunciamiento recogido en la SAN de 29/11/2013 (Rec. 455/2011) referente a los supuestos en los que el denunciado ha adoptado las medidas correctoras oportunas, de acuerdo con lo señalado se debe proceder al archivo de las actuaciones.

De acuerdo con lo señalado,

Por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

1.- ARCHIVAR el procedimiento **A/00269/2016** seguido contra ***RSM CORREDURÍA DE SEGUROS, S.A..***, 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, en relación con la denuncia por la infracción del artículo 9 de la LOPD.

2.- NOTIFICAR el presente Acuerdo a ***RSM CORREDURÍA DE SEGUROS, S.A..*** y a D. ***B.B.B.***.

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 reglamento de desarrollo de la LOPD aprobado por el Real Decreto 1720/2007, de 21 diciembre.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en el artículo 123 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución, o, directamente 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 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de esta acto, según lo previsto en el artículo 46.1 del referido texto legal.

Mar España Martí
Directora de la Agencia Española de Protección de Datos