



Expediente Nº: E/04462/2014

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante el **AYUNTAMIENTO DE MADRID** en virtud de denuncia presentada por **SECCION SINDICAL CCOO JUNTAS MUNICIPALES Y DISTRITOS DEL AYTO DE MADRID** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 21 de abril de 2014 tiene entrada en esta Agencia escrito de la **SECCION SINDICAL CCOO JUNTAS MUNICIPALES Y DISTRITOS DEL AYTO DE MADRID** (en adelante el denunciante) comunicando posible infracción a la Ley Orgánica 15/1999 motivada por cámaras de videovigilancia cuyo titular es el **AYUNTAMIENTO DE MADRID** (en adelante el denunciado) instaladas en **JUNTA MUNICIPAL DE DISTRITO DE CHAMARTIN (C/.....1) MADRID**.

El denunciante manifiesta que se han instalado cámaras de videovigilancia en la planta baja de la Junta Municipal donde se ubican los relojes o tornos y dirigidas hacia ellos, sin que exista ningún distintivo informativo con la identificación del responsable. Asimismo se denuncia que ni la plantilla ni a la representación sindical se les ha informado de la existencia de las cámaras.

Adjunta reportaje fotográfico.

SEGUNDO: Tras la recepción de la denuncia la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes extremos:

Con fecha 29 de julio de 2014 se solicita información a la **JUNTA MUNICIPAL DEL DISTRITO DE CHAMARTIN** teniendo entrada en esta Agencia con fecha 21 de agosto de 2014, escrito del AYUNTAMIENTO DE MADRID en el que manifiesta:

1. Se está instalando en la referida sede un sistema de videovigilancia interior, destinado a garantizar la protección tanto de las personas como de los bienes del edificio.
2. El responsable la instalación es el Área de Gobierno de Seguridad y Emergencias del Ayuntamiento de Madrid.
3. De la instalación y mantenimiento del sistema se ocupa la Junta Municipal de Distrito.
4. La responsabilidad del fichero recae en la Secretaría General Técnica del Área de Gobierno de Seguridad y Emergencias.
5. Una vez finalice la instalación y configuración del sistema de videovigilancia, y con anterioridad a su puesta en marcha, el Servicio de Gestión de la

Seguridad en Edificios e Instalaciones (en adelante, el SEGSEIN) procederá a realizar una auditoría final del sistema, instalar los correspondientes carteles informativos en los accesos al edificio (puerta principal y entrada al aparcamiento) y entregar a los responsables de la Junta de Distrito los formularios informativos que deberán ponerse a disposición de los ciudadanos.

Adjunta modelos de cartel informativo utilizados en el Ayuntamiento de Madrid, donde se especifica todo lo requerido en la instrucción, así como modelos de información al ciudadano sobre sus derechos.

6. Adjunta plano de situación de planta baja, segunda y sótano con ubicación de nueve cámaras.
7. La instalación está compuesta por 4 minidomos, ubicados en los dos núcleos de escalera de las plantas baja y segunda; además de 1 domo móvil y 4 cámaras, instalados en el aparcamiento. De estas nueve cámaras, sólo el domo móvil del aparcamiento (cámara 5 en el plano) admite zoom y movimiento.

No se ha previsto la instalación de cámaras en el exterior del edificio.

8. Aporta fotografías de las cámaras y de imágenes captadas en el monitor numeradas de 1 a 9.

Se aprecian imágenes de nueve cámaras: todas interiores que captan imágenes interiores de planta baja segunda y sótano.

9. El sistema de videovigilancia instalado permite tanto la visualización de imágenes como su grabación. Las imágenes se visualizarán en un monitor de 17" pulgadas y se grabarán las 24 horas del día; centralizándose en un grabador de 16 entradas.
10. Aporta fotografía de monitor y grabador situados en puesto de control en la planta baja.
11. El sistema será visualizado por miembros de Policía Municipal.
12. La grabación se realizará sobre soporte en disco duro con formato protegido. El sistema se configurará para que las grabaciones se borren automáticamente antes de los 30 días de existencia.

Sólo puede recuperar grabaciones el personal autorizado del Servicio de Gestión de la Seguridad en Edificios e Instalaciones (SEGSEIN), del Área de Gobierno de Seguridad y Emergencias.

El acceso a la aplicación informática que gestiona este proceso se realiza mediante control de acceso lógico (Usuario y Password).

Existe un protocolo muy estricto para la cesión de imágenes, que pasa por su petición por escrito al SEGSEIN, especificando de forma clara las motivaciones. Desde este Servicio se evalúa la solicitud para comprobar si dicha cesión se encuadra dentro de los casos previstos en la Ley Orgánica 15/1 999 y si su finalidad es GARANTIZAR LA SEGURIDAD de la sede. En caso afirmativo, se recupera la grabación, se entrega al solicitante y se realiza la anotación correspondiente en el registro de cesiones del documento de seguridad del fichero.

13. El fichero de datos se denomina VIDEOVIGILANCIA SEDES AYUNTAMIENTO DE MADRID cuya finalidad es: garantizar la seguridad de

las sedes del Ayuntamiento de Madrid mediante la videovigilancia perimetral y de los accesos, tanto exteriores como interiores, de las mismas.

14. Según lo aportado en el expediente relacionado E/04529/2014, en lo relativo a este fichero de datos, con motivo del Acuerdo 9 de octubre de 2014 de la Junta de Gobierno de la Ciudad de Madrid, por el que se modifica el Acuerdo de 17 de enero de 2013 por el que se establece la organización y estructura del Área de Gobierno de Seguridad y Emergencias y se delegan competencias en su titular y en los titulares de los órganos directivos, ha cambiado la titularidad del mismo, como ya ha comunicado a la Agencia Española de Protección de Datos el Servicio de Protección de Datos del Ayuntamiento de Madrid; siendo el nuevo Órgano responsable del fichero: el Área de Gobierno de Seguridad y Emergencias, Dirección General de Policía Municipal.
15. Mediante una diligencia en el citado expediente se ha comprobado la inscripción en el RGPD de este fichero con nº *****CÓD.1** cuyo responsable está encuadrado en el Ayuntamiento de Madrid, Área de Gobierno de Seguridad y Emergencias y como Órgano responsable figura:
 - a. la Secretaría General Técnica en la versión 6 de 24/03/2014 y
 - b. la Dirección General de la Policía Municipal en la versión 8 de 03/03/2015
16. En diligencia telefónica del expediente citado con el Área responsable del Ayuntamiento, el representante de la entidad manifiesta que las cámaras instaladas son solo para seguridad del edificio, bienes y personas y no se utilizan para control de trabajadores.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver el Director de la Agencia Española de Protección de Datos, conforme a lo establecido en el artículo 37.d) en relación con el artículo 36, ambos de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD).

II

En primer lugar procede situar el contexto normativo en materia de videovigilancia. Así 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 LOPD, el artículo 2.1 de la misma señala: *“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 apartado a) del artículo 3 de la LOPD, como *“Cualquier información concerniente a personas físicas identificadas o identificables”*.

El artículo 3 de la LOPD define en su letra c) el tratamiento de datos como

aquellas “operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias”.

El artículo 5.1. f) del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, define datos de carácter personal como: *“Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, 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 de octubre de 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, según el cual, a efectos de dicha Directiva, 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”.* Asimismo, el Considerando 26 de esta Directiva se refiere a esta cuestión señalando que, para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona para identificar a aquélla.

La Exposición de Motivos de la Instrucción 1/2006, de 8 de noviembre, de esta Agencia Española de Protección de Datos, relativa al tratamiento de los datos con fines de videovigilancia señala que: *“La seguridad y la vigilancia, elementos presentes en la sociedad actual, no son incompatibles con el derecho fundamental a la protección de la imagen como dato personal, lo que en consecuencia exige respetar la normativa existente en materia de protección de datos, para de esta manera mantener la confianza de la ciudadanía en el sistema democrático”.* Sigue señalando: *“Las imágenes se consideran un dato de carácter personal, en virtud de lo establecido en el artículo 3 de la Ley Orgánica 15/1999...”.*

La garantía del derecho a la protección de datos, conferida por la normativa de referencia, requiere que exista una actuación que constituya un tratamiento de datos personales en el sentido expresado. En otro caso las mencionadas disposiciones no serán de aplicación.

Por su parte, la citada Instrucción 1/2006, dispone en su artículo 1.1 lo siguiente:

“1. La presente Instrucción se aplica al tratamiento de datos personales de imágenes de personas físicas identificadas o identificables, con fines de vigilancia a través de sistemas de cámaras y videocámaras.

El tratamiento objeto de esta Instrucción comprende la grabación, captación, transmisión, conservación, y almacenamiento de imágenes, incluida su reproducción o emisión en tiempo real, así como el tratamiento que resulte de los datos personales relacionados con aquéllas.

Se considerará identificable una persona cuando su identidad pueda determinarse mediante los tratamientos a los que se refiere la presente instrucción, sin que ello

requiera plazos o actividades desproporcionados.

Las referencias contenidas en esta Instrucción a videocámaras y cámaras se entenderán hechas también a cualquier medio técnico análogo y, en general, a cualquier sistema que permita los tratamientos previstos en la misma.” (el subrayado es de la Agencia Española de Protección de Datos).

La Instrucción 1/2006 en su artículo 2 establece lo siguiente:

“1. Sólo será posible el tratamiento de los datos objeto de la presente instrucción, cuando se encuentre amparado por lo dispuesto en el artículo 6.1 y 2 y el artículo 11.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

2. Sin perjuicio de lo establecido en el apartado anterior la instalación de cámaras y videocámaras deberá respetar en todo caso los requisitos exigidos por la legislación vigente en la materia.”

De lo anteriormente expuesto se desprende que el concepto de dato personal, según la definición de la LOPD, requiere la concurrencia de un doble elemento: por una parte, la existencia de una información o dato y, por otra, que dicho dato pueda vincularse a una persona física identificada o identificable, por lo que la imagen de una persona física identificada o identificable constituye un dato de carácter personal.

De acuerdo con los preceptos transcritos, la cámara reproduce la imagen de los afectados por este tipo de tratamientos y, a efectos de la LOPD, la imagen de una persona constituye un dato de carácter personal, toda vez que la información que capta concierne a personas que las hacen identificadas o identificables y suministra información sobre la imagen personal de éstas, el lugar de su captación y la actividad desarrollada por el individuo al que la imagen se refiere.

III

En el presente expediente se denuncia por parte del representante de la Sección Sindical de Comisiones Obreras de Juntas Municipales y Distritos del Ayuntamiento de Madrid, la instalación de un sistema de videovigilancia en la Junta Municipal del Distrito de Chamartín, que pudiera contravenir la normativa de protección de datos en diversos aspectos tales como la falta de información a los órganos de representación de los empleados, ni a los empleados o la inexistencia de cartel informativo de la existencia de las cámaras.

Ahora bien, en esta cuestión, en primer lugar se plantea si es necesario el consentimiento inequívoco de los trabajadores cuando se instalan cámaras de videovigilancia en el centro de trabajo, al amparo del artículo 6.1 de la LOPD.

A este respecto es necesario realizar varias aclaraciones respecto al consentimiento en el ámbito laboral. Así, el consentimiento, elemento base en el tratamiento de los datos, entraña cierta complejidad, especialmente cuando nos referimos al ámbito laboral, dado que resulta de difícil cumplimiento que en ese ámbito concurren los requisitos legalmente previstos para considerar que se ha obtenido

libremente el consentimiento. El artículo 3 h) de la LOPD lo define como *“Toda manifestación de voluntad libre, inequívoca, específica e informada mediante la que el interesado consienta el tratamiento de datos personales que el conciernen”*.

Del concepto de consentimiento se desprende la necesaria concurrencia para que el mismo pueda ser considerado conforme a derecho de los cuatro requisitos enumerados en dicho precepto. Un adecuado análisis del concepto exigirá poner de manifiesto cuál es la interpretación que ha de darse a estas cuatro notas características del consentimiento, tal y como la misma ha indicado en numerosas Resoluciones de la AEPD, siguiendo a tal efecto los criterios sentados en las diversas recomendaciones emitidas por el Comité de Ministros del Consejo de Europa en relación con la materia que nos ocupa. A la luz de dichas recomendaciones, el consentimiento habrá de ser:

a) Libre, lo que supone que el mismo deberá haber sido obtenido sin la intervención de vicio alguno del consentimiento en los términos regulados por el Código Civil.

b) Específico, es decir referido a un determinado tratamiento o serie de tratamientos concretos y en el ámbito de las finalidades determinadas, explícitas y legítimas del responsable del tratamiento, tal y como impone el artículo 4.2 de la LOPD.

c) Informado, es decir que el afectado conozca con anterioridad al tratamiento la existencia del mismo y las finalidades para las que el mismo se produce. Precisamente por ello el artículo 5.1 de la LOPD impone el deber de informar a los interesados de una serie de extremos que en el mismo se contienen.

d) Inequívoco, lo que implica que no resulta admisible deducir el consentimiento de los meros actos realizados por el afectado (consentimiento presunto), siendo preciso que exista expresamente una acción u omisión que implique la existencia del consentimiento.

La concurrencia de estos requisitos resulta de difícil cumplimiento en el ámbito laboral. En consecuencia, vista la dificultad que entraña obtener el consentimiento, la Agencia Española de Protección de Datos, ha entendido que lo procedente es acudir a las normas que legitimen el tratamiento de los datos. Por tanto, en el ámbito laboral, el Ordenamiento Jurídico Español, regula en el Estatuto de los Trabajadores, aprobado por Real Decreto Legislativo de 24 de Octubre de 1995, los poderes de Dirección del empresario y es en éste articulado donde hallamos la oportuna legitimación.

El artículo 20.3 del Estatuto de los Trabajadores (ET) dispone que *“El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso”*.

De todo ello se desprende que el empresario, se haya legitimado para tratar las imágenes de sus trabajadores en el ámbito laboral, al amparo del artículo 20.3 del ET. Ahora bien, esta legitimación no es absoluta y exige por parte del empresario la obligación de informar de dicho tratamiento a los trabajadores (cumpliendo así con el deber de informar previsto tanto en el artículo 10 de la Directiva 95/46/CE como en el artículo 5 de la LOPD.).

Sin embargo, en el caso que nos ocupa, el representante del Ayuntamiento ha manifestado que la finalidad del sistema de videovigilancia es garantizar la protección tanto de las personas como los bienes del edificio, sin que conste ni se aporten pruebas al respecto que acrediten que el sistema de videovigilancia vaya a ser utilizado para fines distintos que no sean los de seguridad de las instalaciones y del personal de la misma, por lo tanto no existiría una finalidad de control de los trabajadores.

Es necesario en este punto diferenciar si la instalación de la cámara en el centro de trabajo es como medida de vigilancia y control del empresario, para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales o si es una medida de seguridad para proteger la instalación y sus empleados (como es el caso que nos ocupa).

En el primer caso, es decir cuando el objetivo de la instalación de las cámaras va dirigido al cumplimiento por los trabajadores de sus deberes laborales, se aplicaría toda la normativa y jurisprudencia recogida "ut supra", es decir sería necesario por parte del empresario, garantizar el derecho de información en la recogida de las imágenes, mediante información a los trabajadores del alcance específico que se va a dar a las mismas para el control laboral.

En el segundo caso, es decir cuando la finalidad es de vigilancia y protección de las instalaciones y personal de la empresa, es necesario el cumplimiento de la LOPD, el Reglamento de Desarrollo de la LOPD y la Instrucción 1/2006. Por lo tanto, debería cumplirse, entre otros, el deber de información recogido en el artículo 5 de la LOPD, disponiendo de distintivos informativos de zona de videovigilancia acordes a la Instrucción 1/2006 e impresos informativos.

A este respecto, cabe decir que solicitada información a la entidad denunciada, por los Servicios de Inspección de esta Agencia, manifiestan que a la fecha de solicitud de información en julio de 2014, el sistema se encontraba en proceso de instalación no habiendo finalizado el mismo y una vez que finalizase la instalación y configuración del sistema de videovigilancia, y con anterioridad a su puesta en marcha, el Servicio de Gestión de la Seguridad en Edificios e Instalaciones (en adelante, el SEGSEIN) procedería a realizar una auditoría final del sistema, instalar los correspondientes carteles informativos en los accesos al edificio (puerta principal y entrada al aparcamiento) y entregar a los responsables de la Junta de Distrito los formularios informativos que deberán ponerse a disposición de los ciudadanos.

Se aportan modelo de cartel informativo, utilizado en el Ayuntamiento de Madrid, que se instalarán una vez se finalice la instalación que resultan acordes al artículo 3 a) de la Instrucción 1/2006, en relación al artículo 5 de la LOPD. Asimismo se aporta modelo de folleto informativo que se pondrá a disposición de los interesados, de conformidad con el artículo 3 b) de la citada Instrucción.

Por otro lado, respecto al cumplimiento de la inscripción de ficheros, el artículo 26.1 de la LOPD, recoge lo siguiente:

"1. Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos"

El responsable del fichero es el titular del fichero que contiene datos de carácter personal. Sobre él van a recaer las obligaciones que establece la LOPD. . El

responsable del fichero, antes de disponerse a someter datos personales a tratamiento, deberá cumplir con los requisitos de la normativa de protección de datos, teniendo en cuenta su naturaleza y la naturaleza de los datos que va a someter a tratamiento.

El apartado d) del artículo 3 de la LOPD define al responsable del fichero o tratamiento como aquella persona física o jurídica, de naturaleza pública o privada, u órgano administrativo que decida sobre la finalidad, contenido y uso del tratamiento. El artículo 43 de la LOPD sujeta a su régimen sancionador precisamente al responsable del fichero o tratamiento.

El reglamento de desarrollo de la LOPD, aprobado por RD 1720/2007, de 21 de diciembre, complementa esta definición en el apartado q) del artículo 5, en el que señala lo siguiente:

“q) Responsable del fichero o del tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que solo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.

Podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados”.

El responsable del fichero es, en suma, quien debe garantizar el derecho fundamental de protección de datos personales de todas las personas cuyos datos almacena. Por ello, va a estar obligado a llevar a cabo una serie de actuaciones dirigidas a la protección de los datos, a su integridad y a su seguridad.

El responsable debe notificar su fichero a la Agencia Española de Protección de Datos, que dispondrá inscribirlo en el Registro General de Protección de Datos. La notificación de inscripción del fichero facilitará que terceros puedan conocer que se está produciendo un tratamiento con una finalidad determinada y los afectados tendrán la oportunidad de ejercitar sus derechos ante el responsable.

Además este es el criterio que se hace constar en la Instrucción 1/2006 , al señalar en su artículo 7 que *“1-La persona o entidad que prevea la creación de ficheros de videovigilancia deberá notificarlo previamente a la Agencia Española de Protección de Datos, para su inscripción en el Registro General de la misma.*

Tratándose de ficheros de titularidad pública deberá estarse a lo establecido en el artículo 20 de la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal.

2.-A estos efectos, no se considerará fichero el tratamiento consistente exclusivamente en la reproducción o emisión de imágenes en tiempo real.”

El artículo 20.1 de la LOPD, establece que la creación, modificación o supresión de ficheros de las Administraciones Públicas sólo podrán hacerse por medio de disposición general publicada en el Boletín Oficial del Estado o Diario Oficial correspondiente. Por su parte el artículo 53.1 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, determina que cuando la disposición se refiera a los órganos de la Administración General del

Estado o a las entidades u organismos vinculados o dependientes de la misma, deberá revestir la forma de orden ministerial o resolución del titular de la entidad u organismo correspondiente.

Según lo aportado en el expediente relacionado E/04529/2014, en lo relativo a este fichero de datos, con motivo del Acuerdo 9 de octubre de 2014 de la Junta de Gobierno de la Ciudad de Madrid, por el que se modifica el Acuerdo de 17 de enero de 2013 por el que se establece la organización y estructura del Área de Gobierno de Seguridad y Emergencias y se delegan competencias en su titular y en los titulares de los órganos directivos, ha cambiado la titularidad del mismo, como ya ha comunicado a la Agencia Española de Protección de Datos el Servicio de Protección de Datos del Ayuntamiento de Madrid; siendo el nuevo Órgano responsable del fichero: el Área de Gobierno de Seguridad y Emergencias, Dirección General de Policía Municipal.

Así, consta la inscripción del fichero denominado "VIDEOVIGILANCIA SEDES AYUNTAMIENTO MADRID" en el Registro de Protección de Datos de esta Agencia, en fecha 11/01/2008, siendo su última modificación el 03/03/2015, figurando actualmente como responsable la Dirección General de la Policía Municipal.

Las imágenes se almacenan por un periodo máximo de 30 días, de conformidad al artículo 6 de la citada Instrucción 1/2006.

Por lo tanto, a la vista de todo lo expuesto, en el presente caso no se aprecia vulneración de la normativa aplicable en materia de videovigilancia, por lo que procede el archivo del presente expediente de actuaciones previas.

Por lo tanto, de acuerdo con lo señalado,

Por el Director de la Agencia Española de Protección de Datos,

SE ACUERDA:

1. **PROCEDER AL ARCHIVO** de las presentes actuaciones.
2. **NOTIFICAR** la presente Resolución a **AYUNTAMIENTO DE MADRID** y a **SECCION SINDICAL CCOO JUNTAS MUNICIPALES Y DISTRITOS DEL AYTO DE MADRID**.

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 (artículo 48.2 de la LOPD), y de conformidad con lo establecido 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, los interesados podrán interponer, potestativamente, recurso de reposición ante el Director 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 este acto, según lo previsto en el artículo 46.1 del referido texto legal.

Sin embargo, el responsable del fichero de titularidad pública, de acuerdo con el artículo 44.1 de la citada LJCA, sólo podrá interponer 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 LJCA, 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 del referido texto legal.

José Luis Rodríguez Álvarez
Director de la Agencia Española de Protección de Datos