

- **Expediente N.º: EXP202206481**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

Del procedimiento instruido por la Agencia Española de Protección de Datos y en base a los siguientes

ANTECEDENTES

PRIMERO: Con fecha 6 de junio de 2022 **A.A.A.** (en adelante, la parte reclamante) interpuso reclamación ante la Agencia Española de Protección de Datos.

La reclamación se dirige contra **HERON CITY VALENCIA MANAGEMENT S.L.** con NIF-**B83122937** (en adelante, la parte reclamada).

Los motivos en que basa la reclamación son los siguientes: en fecha 6 de junio de 2022, mediante correo electrónico que aporta junto a su reclamación, solicitó a la parte reclamada, tras haber intentado realizar su solicitud de forma presencial en las instalaciones de la parte reclamada, acceso a imágenes procedentes del sistema de videovigilancia ubicado en sus instalaciones, recibiendo respuesta que aporta, en la que la parte reclamada señala que no cabe dicho acceso, sino cuando exista previa denuncia, siendo solicitados por la Policía o personal autorizado, entendiéndose la parte reclamante que dicha respuesta no es conforme a la normativa de protección de datos.

SEGUNDO: Con fecha 12 de julio de 2022, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la parte reclamante.

TERCERO: Con fecha 30 de agosto de 2022, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la parte reclamada, con arreglo a lo dispuesto en los artículos 63 y 64 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), por la presunta infracción del Artículo 15 del RGPD, tipificada en el Artículo 83.5 del RGPD.

CUARTO: Notificado el citado acuerdo de inicio conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), la parte reclamada presentó escrito de alegaciones en el que, en síntesis, manifestaba que entre sus funciones no se encuentra el sistema de videovigilancia y el tratamiento de los datos de carácter personal captados a través de dicho sistema.

Manifiesta además que no le consta que el reclamante se personara en sus oficinas ni que trasladara personal o telefónicamente su intención de ejercer ningún derecho (cuestión, por otro lado, que tampoco el reclamante acredita de ninguna forma), sí es cierto que dirigió una comunicación electrónica a la dirección de correo electrónico marketing@heroncityvalencia.com anunciando que en caso de no facilitarle “el acceso a grabaciones en las que estoy grabado en su centro comercial” lo pondría en conocimiento de esta Agencia.

En este sentido señala que la dirección de correo electrónico a la que el interesado se dirigió no guarda relación con el tratamiento de datos de carácter personal ni con los medios de contacto habilitados para el ejercicio de los derechos de los interesados en el marco del centro comercial en cuestión.

QUINTO: Con fecha 21 de septiembre de 2022, el instructor del procedimiento acordó practicar las siguientes pruebas dándose por reproducidos a efectos probatorios la reclamación interpuesta por **A.A.A.** y su documentación, los documentos obtenidos y generados durante la fase de admisión a trámite de la reclamación, y el informe de actuaciones previas de investigación que forman parte del procedimiento AT/02740/2022.

Asimismo, se da por reproducido a efectos probatorios, las alegaciones al acuerdo de inicio del procedimiento sancionador referenciado, presentadas por **HERON CITY VALENCIA MANAGEMENT, S.L.**, y la documentación que a ellas acompaña.

SEXTO: Con fecha 26 de septiembre de 2022 se formuló propuesta de resolución, proponiendo que por la Directora de la Agencia Española de Protección de Datos se sancione a **HERON CITY VALENCIA MANAGEMENT, S.L.**, con NIF **B83122937**, por una infracción del artículo 15 del RGPD, tipificada en el artículo 83.5 del RGPD, con una multa de 10.000 € (diez mil euros)

SEPTIMO: Con fecha 10 de octubre de 2020, en respuesta a la propuesta de resolución dictada, la entidad reclamada presentó alegaciones señalando que se ha puesto en contacto con **HERON CITY MEDITERRÁNEO, S.L.**, la cual afirma tener un contrato de prestación de servicios con una empresa gestora del mantenimiento de la instalación de los equipos del CCTV (circuito cerrado de televisión) del Centro Comercial de Heron City de Paterna.

En virtud de dicho contrato, tanto **HERON CITY MEDITERRÁNEO, S.L.** -en calidad de responsable del tratamiento de los datos obtenidos de la actividad de videovigilancia- como la empresa contratada -en calidad de encargado del tratamiento- son las únicas entidades con acceso a los datos personales objeto de este expediente.

Pese a que ambas entidades, **HERON CITY VALENCIA MANAGEMENT, S.L.**, y **HERON CITY MEDITERRÁNEO, S.L.**, pertenecen al mismo grupo empresarial, la entidad reclamada manifiesta que no está facultada para aportar a este procedimiento copia de dicho contrato.

De las actuaciones practicadas en el presente procedimiento y de la documentación obrante en el expediente, han quedado acreditados los siguientes:

HECHOS PROBADOS

PRIMERO: El 6 de junio de 2022 el reclamante solicita el acceso a las imágenes procedentes del sistema de videovigilancia ubicado en sus instalaciones, y la parte reclamada le responde a su correo electrónico desde marketing@heroncityvalencia.com de la siguiente manera:

“Le indicamos que las imágenes de las cámaras de videovigilancia sólo se pueden requerir por personal autorizado o la policía, y sólo en el caso de que exista una denuncia previa, por lo que le recomendamos que ponga la denuncia.

No obstante, le indicamos que las cámaras no están continuamente grabando, graban por periodos de tiempo.

En caso que nos lo solicite la policía, necesitaríamos saber la fecha, ubicación exacta y tramo horario lo más estrecho posible para es si existe una grabación en ese periodo.

También le indicamos que las grabaciones se autodestruyen a los 15 días si no hay ningún requerimiento policial.”

SEGUNDO. Como consecuencia de lo anterior, esta Agencia considera que no fue respetado el derecho de acceso de la parte reclamante a sus datos personales, conforme establece el artículo 15 del RGPD.

FUNDAMENTOS DE DERECHO

I

De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada autoridad de control y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), es competente para iniciar y resolver este procedimiento la Directora de la Agencia Española de Protección de Datos.

Asimismo, el artículo 63.2 de la LOPDGDD determina que: "Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos."

II

La imagen física de una persona, a tenor del artículo 4.1 del RGPD, es un dato personal y su protección, por tanto, es objeto de dicho Reglamento. En el artículo 4.2 del RGPD se define el concepto de "tratamiento" de datos personales.

Las imágenes generadas por un sistema de cámaras o videocámaras son datos de carácter personal, por lo que su tratamiento está sujeto a la normativa de protección de datos.

Es, por tanto, pertinente analizar si el tratamiento de datos personales (imagen de las personas físicas) llevado a cabo a través del sistema de videovigilancia denunciado es acorde con lo establecido en el RGPD.

III

El artículo 6.1 del RGPD establece los supuestos que permiten considerar lícito el tratamiento de datos personales.

En cuanto al tratamiento con fines de videovigilancia, el artículo 22 de la LOPDGDD establece que las personas físicas o jurídicas, públicas o privadas, podrán llevar a cabo el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones.

El artículo 15 del RGPD, reconoce el derecho de acceso señalando lo siguiente:

“1. El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a la siguiente información:

a) los fines del tratamiento;

b) las categorías de datos personales de que se trate;

c) los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales;

d) de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo;

e) la existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento;

f) el derecho a presentar una reclamación ante una autoridad de control;

g) cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen;

h) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

2. Cuando se transfieran datos personales a un tercer país o a una organización internacional, el interesado tendrá derecho a ser informado de las garantías adecuadas en virtud del artículo 46 relativas a la transferencia.

3. El responsable del tratamiento facilitará una copia de los datos personales objeto de tratamiento. El responsable podrá percibir por cualquier otra copia solicitada por el in-

interesado un canon razonable basado en los costes administrativos. Cuando el interesado presente la solicitud por medios electrónicos, y a menos que este solicite que se facilite de otro modo, la información se facilitará en un formato electrónico de uso común.

4. El derecho a obtener copia mencionado en el apartado 3 no afectará negativamente a los derechos y libertades de otros.”

IV

De conformidad con lo expuesto, el tratamiento de imágenes a través de un sistema de videovigilancia, para ser conforme con la normativa vigente, debe cumplir los requisitos siguientes:

1.- La personas físicas o jurídicas, públicas o privadas, pueden establecer un sistema de videovigilancia con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones.

Se ha de valorar si la finalidad pretendida puede lograrse de otra forma menos intrusiva para los derechos y libertades de los ciudadanos. Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios, considerando 39 del RGPD.

2.- Las imágenes obtenidas no puedan utilizarse para una finalidad ulterior incompatible con la que motivó la instalación del sistema de videovigilancia.

3.- Se deberá cumplir con el deber de informar a los afectados previsto en los artículos 12 y 13 del RGPD, y 22 de la LOPDGDD.

En tal sentido, el artículo 22 de la LOPDGDD prevé en relación con la videovigilancia un sistema de “información por capas”.

La primera capa ha de referirse, al menos, a la existencia del tratamiento (videovigilancia), la identidad del responsable, la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del RGPD y dónde obtener más información sobre el tratamiento de los datos personales.

Esta información se contendrá en un dispositivo colocado en un lugar suficientemente visible y debe suministrarse por adelantado.

La información de la segunda capa debe estar disponible en un lugar fácilmente accesible al afectado, ya sea una hoja informativa en una recepción, cajero, etc..., colocada en un espacio público visible o en una dirección web, y ha de referirse al resto de elementos del artículo 13 del RGPD.

4.- No pueden captarse imágenes de la vía pública, puesto que el tratamiento de imágenes en lugares públicos, salvo que concurra autorización gubernativa, sólo puede ser realizado por las Fuerzas y Cuerpos de Seguridad.

En algunas ocasiones, para la protección de espacios privados, donde se hayan instalado cámaras en fachadas o en el interior, puede ser necesario para garantizar la finalidad de seguridad la grabación de una porción de la vía pública.

Es decir, las cámaras y videocámaras instaladas con fines de seguridad no podrán obtener imágenes de la vía pública salvo que resulte imprescindible para dicho fin, o resulte imposible evitarlo por razón de la ubicación de aquéllas. Y, en tal caso extraordinario, las cámaras sólo podrán captar la porción mínima necesaria para preservar la seguridad de las personas y bienes, así como de sus instalaciones.

Las cámaras instaladas no pueden obtener imágenes de espacio privativo de tercero y/o espacio público sin causa justificada debidamente acreditada, ni pueden afectar a la intimidad de transeúntes que transiten libremente por la zona.

No está permitida, por tanto, la colocación de cámaras hacia la propiedad privada de vecinos con la finalidad de intimidarlos o afectar a su ámbito privado sin causa justificada.

En ningún caso se admitirá el uso de prácticas de vigilancia más allá del entorno objeto de la instalación y en particular, no pudiendo afectar a los espacios públicos circundantes, edificios contiguos y vehículos distintos de los que accedan al espacio vigilado.

No pueden captarse ni grabarse imágenes en espacios propiedad de terceros sin el consentimiento de sus titulares, o, en su caso, de las personas que en ellos se encuentren.

Resulta desproporcionado captar imágenes en espacios privados, tales como vestuarios, taquillas o zonas de descanso de trabajadores.

5.- Las imágenes podrán conservarse por un plazo máximo de un mes, salvo en aquellos supuestos en que se deban conservar para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones.

En este segundo supuesto, deberán ser puestas a disposición de la autoridad competente en un plazo máximo de 72 horas desde que se tuviera conocimiento de la existencia de la grabación.

6.- El responsable deberá llevar un registro de actividades de los tratamientos efectuados bajo su responsabilidad en el que se incluya la información a la que hace referencia el artículo 30.1 del RGPD.

7.- El responsable deberá realizar un análisis de riesgos o, en su caso, una evaluación de impacto en la protección de datos, para detectar los derivados de la implantación del sistema de videovigilancia, valorarlos y, en su caso, adoptar las medidas de seguridad apropiadas.

8.- Cuando se produzca una brecha de seguridad que afecte a los tratamientos de cámaras con fines de seguridad, siempre que exista riesgo para los derechos y

libertades de las personas físicas, deberá notificarlo a la AEPD en un plazo máximo de 72 horas.

Se entiende por brecha de seguridad la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizado a dichos datos.

9.- Cuando el sistema esté conectado a una central de alarma, únicamente podrá ser instalado por una empresa de seguridad privada que reúna los requisitos contemplados en el artículo 5 de la Ley 5/2014 de Seguridad Privada, de 4 de abril.

La Agencia Española de Protección de Datos ofrece a través de su página web [<https://www.aepd.es>] acceso a:

- la legislación en materia de protección de datos personales, incluyendo el RGPD y la LOPDGDD (apartado “Informes y resoluciones” / “normativa”),
- la Guía sobre el uso de videocámaras para seguridad y otras finalidades,
- la Guía para el cumplimiento del deber de informar (ambas disponibles en el apartado “Guías y herramientas”).

También resulta de interés, en caso de realizar tratamientos de datos de bajo riesgo, la herramienta gratuita Facilita (en el apartado “Guías y herramientas”), que, mediante unas preguntas concretas, permite valorar la situación del responsable respecto del tratamiento de datos personales que lleva a cabo, y en su caso, generar diversos documentos, cláusulas informativas y contractuales, así como un anexo con medidas de seguridad orientativas consideradas mínimas.

V

En el presente caso se deniega el derecho de acceso al reclamante, manifestando no falta de competencia o de tratamiento de tales datos como ha expresado en las alegaciones remitidas a esta Agencia, sino que le indica al reclamante que se le deniega el acceso a las mismas porque según la entidad reclamada sólo tienen derecho de acceso a las grabaciones personal autorizado o la policía.

De tales afirmaciones se desprende que la entidad reclamada reconoce que lleva a cabo grabaciones y por tanto es responsable del tratamiento de datos personales, en concreto de la imagen, y que en este caso se le deniega el derecho de acceso al reclamante.

A lo largo del procedimiento, la entidad reclamada alega no ser la entidad responsable, y afirma no poder aportar el documento que lo constata pese a señalar que la responsable es otra entidad de su mismo grupo empresarial.

En este sentido señalar, que los encargados del tratamiento tienen la obligación de asistir al responsable, teniendo en cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III, según dispone el artículo 28.3.e) del RGPD. Esta obligación incumbe a todos los encargados

formen parte o no del grupo empresarial del responsable y en el contrato se debe estipular cómo el encargado del tratamiento prestará esa asistencia al responsable.

En este caso no conocemos que tipo de asistencia se ha pactado ni siquiera el reclamado acredita que actúe como encargado del tratamiento y aun en el caso de actuar como encargado del tratamiento, la entidad reclamada debió al menos trasladar la solicitud de acceso al responsable, ya que la evaluación de si las solicitudes de los interesados son admisibles o si se cumplen los requisitos establecidos por el RGPD debe ser realizada por el responsable del tratamiento, como recogen las Directrices 07/2020 sobre los conceptos de responsable y encargado en el RGPD. Versión 2.0. adoptado el 07 de julio de 2021.

Así las cosas, aunque la entidad reclamada fuera encargada sería responsable de la infracción ya que tomó la decisión de no facilitar al reclamante el acceso a la grabación en lugar de trasladarla al responsable

Por lo tanto, se considera que los hechos expuestos, es decir, no dar acceso al reclamante a las grabaciones que se realizaron sobre él y su vehículo en las instalaciones del demandado, y no poder acreditar su falta de responsabilidad, se considera que se ha vulnerado el artículo 15 del RGPD, lo que supone la comisión de una infracción tipificada en el artículo 83.5 del RGPD, que dispone lo siguiente:

“Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

b) los derechos de los interesados a tenor de los artículos 12 a 22; (...).”

A efectos del plazo de prescripción de las infracciones, la infracción señalada en el párrafo anterior se considera muy grave conforme al artículo 72.1 de la LOPDGDD, que establece que:

“En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

(...)

k) El impedimento o la obstaculización o la no atención reiterada del ejercicio de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679.”

VI

La multa que se imponga deberá ser, en cada caso individual, efectiva, proporcionada y disuasoria, conforme a lo establecido en el artículo 83.1 del RGPD.

Por tanto, procede graduar la sanción a imponer de acuerdo con los criterios que establece el artículo 83.2 del RGPD, y con lo dispuesto en el artículo 76 de la LOPDGDD, respecto al apartado k) del citado artículo 83.2 RGPD.

El artículo 83.2 del RGPD establece que:

“Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j).

Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:

a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;

b) la intencionalidad o negligencia en la infracción;

c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;

d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;

e) toda infracción anterior cometida por el responsable o el encargado del tratamiento;

f) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;

g) las categorías de los datos de carácter personal afectados por la infracción;

h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida;

i) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;

j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42, y

k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción.”

En el presente caso, se han tenido en cuenta, como agravante la clara intencionalidad de la entidad reclamada para la comisión de los hechos objeto de este procedimiento sancionador, según el artículo 83.2 b) del RGPD, al no ser permitido el acceso por parte de la entidad reclamada, a las imágenes de grabación de la imagen del denunciante y su vehículo, ni tampoco señalar ante quién podría ejercer tales derechos, en el caso de que tales servicios estuviesen encomendados a otra empresa perteneciente al mismo grupo empresarial, como ha señalado en sus alegaciones.

Por todo ello, se considera que la sanción que correspondería imponer sería de 10.000 euros.

Por lo tanto, de acuerdo con la legislación aplicable y valorados los criterios de graduación de las sanciones cuya existencia ha quedado acreditada,

la Directora de la Agencia Española de Protección de Datos **RESUELVE**:

PRIMERO: IMPONER a **HERON CITY VALENCIA MANAGEMENT, S.L.**, con NIF **B83122937**, por una infracción del artículo 15 del RGPD, tipificada en el artículo 83.5 del RGPD, una multa de 10.000 euros (diez mil euros).

SEGUNDO: NOTIFICAR la presente resolución a **HERON CITY VALENCIA MANAGEMENT, S.L.**

TERCERO: Advertir al sancionado que deberá hacer efectiva la sanción impuesta una vez que la presente resolución sea ejecutiva, de conformidad con lo dispuesto en el art. 98.1.b) de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante LPACAP), en el plazo de pago voluntario establecido en el art. 68 del Reglamento General de Recaudación, aprobado por Real Decreto 939/2005, de 29 de julio, en relación con el art. 62 de la Ley 58/2003, de 17 de diciembre, mediante su ingreso, indicando el NIF del sancionado y el número de procedimiento que figura en el encabezamiento de este documento, en la cuenta restringida nº **ES00 0000 0000 0000 0000 0000**, abierta a nombre de la Agencia Española de Protección de Datos en la entidad bancaria CAIXABANK, S.A.. En caso contrario, se procederá a su recaudación en período ejecutivo.

Recibida la notificación y una vez ejecutiva, si la fecha de ejecutividad se encuentra entre los días 1 y 15 de cada mes, ambos inclusive, el plazo para efectuar el pago voluntario será hasta el día 20 del mes siguiente o inmediato hábil posterior, y si se encuentra entre los días 16 y último de cada mes, ambos inclusive, el plazo del pago será hasta el 5 del segundo mes siguiente o inmediato hábil posterior.

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez haya sido notificada a los interesados.

Contra esta resolución, que pone fin a la vía administrativa conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, 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 este acto, según lo previsto en el artículo 46.1 de la referida Ley.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) de la LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la Agencia Española de Protección de Datos, presentándolo a través del Registro Electrónico de la Agencia [<https://sedeagpd.gob.es/sede-electronica-web/>], o a través de alguno de los restantes registros previstos en el art. 16.4 de la citada Ley 39/2015, de 1 de octubre. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

938-120722

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