- **Expediente N.º: PS/00571/2021**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: D. ***A.A.A.*** (en adelante, la parte reclamante), con fecha 3 de enero de 2021, interpuso ante la Agencia Española de Protección de Datos, reclamación contra el AYUNTAMIENTO DE FUENLABRADA, con NIF P2805800F (en adelante, el AYUNTAMIENTO).

La parte reclamante pone en conocimiento de esta Agencia Española de Protección de Datos que el AYUNTAMIENTO ha enviado un correo electrónico "sin copia oculta" a una pluralidad de personas inscritas en la "lista Municipal del ***XXXXXX***", así como que en dicho correo electrónico se adjuntaba un documento que incluía un listado con los datos personales (nombre, apellidos, y DNI) de estas personas.

Junto a la reclamación aporta:

- Copia del correo electrónico dirigido por el reclamado (el origen del correo consignado en el mismo correspondería con el nombre y apellidos del empleado del reclamado que lo habría enviado) a los afectados (incluye, dentro del apartado "Para" un conjunto de direcciones de correo electrónico) con fecha de 20 de noviembre de 2020.

  El asunto del correo electrónico es "Consulta del prelistado de beneficiarios Banco Municipal de ***XXXXXX***".

  El cuerpo del mensaje contiene, entre otros, los siguientes párrafos:

  "*Os remito el listado que se nos ha notificado desde Protección Civil en el que se relacionan todas las personas que han realizado finalmente alguna actividad de BMT hasta el 10 de noviembre.*

  Me gustaría pediros, por favor, que lo consultarais y si hubiera alguien que hubiera realizado la actividad y no apareciera en dicho listado, se pusiera en contacto conmigo mediante un correo electrónico refiriéndome tal incidencia, para poder resolverla.

[…] Esta prelista no es la resolución del expediente, con lo que habría que esperar a la aprobación del expediente en Junta de Gobierno Local y su publicación para llevar a cabo los ingresos de los importes de BMT."

Además se incluye la reseña de contener un adjunto de título "Listado Estudia…da.pdf".

- Copia del documento adjunto al correo electrónico descrito en el punto anterior.

  El documento incluye un listado de personas para cada una de las cuales se facilitan los siguientes valores*: "ORDEN LISTA", "NOMBRE UNIVERSITARIO", "APELLIDO 1", "APELLIDO 2", "DNI".*

SEGUNDO: Con fecha 12 de febrero de 2021, y de conformidad con lo dispuesto en el artículo 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD) se da traslado de dicha reclamación a la parte reclamada, para que procediese a su análisis e informase a esta Agencia en el plazo de un mes, de las acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos.

El 4 de marzo de 2021 consta en esta Agencia contestación al traslado de la reclamación, admitiéndose a trámite la reclamación presentada por la parte reclamante mediante acuerdo de fecha 22 de marzo de ese mismo año.

Como consecuencia del traslado de la reclamación y la solicitud de remisión de información, el AYUNTAMIENTO fue consciente de la brecha de seguridad de datos personales sufrida, procediendo a su notificación a la Agencia Española de Protección de Datos.

TERCERO: Con fecha 24 de febrero de 2021, la Subdirección General de Inspección de Datos recibió para su valoración un escrito de notificación de brecha de seguridad de los datos personales remitido por el AYUNTAMIENTO, recibido en fecha 17 de febrero de 2021, de la que tiene conocimiento cuando se le da traslado de la reclamación presentada por la parte reclamante.

A los efectos oportunos, se informa a la Agencia Española de Protección de Datos de lo siguiente:

(…).

CUARTO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos objeto de la notificación, teniendo conocimiento de los siguientes extremos:

(…).

Con carácter previo al incidente***,*** el AYUNTAMIENTO antes de la implantación del RGPD y desde su aplicación ***(…).***

Inmediatamente después de tener conocimiento del requerimiento de información de la AEPD, tras la presentación de la reclamación***, (…):***

- ***(…).***

QUINTO: Con fecha 5 de enero de 2022, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la parte reclamada, por la presunta infracción de los artículos 5.1 f), 32 y 33 del RGPD, tipificadas en los artículos 83.5 y 83.4 del RGPD.

SEXTO: El AYUNTAMIENTO, en fecha 21 de enero del presente año, presentó escrito de alegaciones al acuerdo de inicio, en el que expone lo siguiente:

> PRIMERO. – ***(…).***
>
> El hecho de que no conste una utilización posterior de la información personal difundida no desvirtúa el hecho de que se ha producido un acceso no autorizado a las direcciones de correo electrónico de todos los participantes en el programa "Banco del ***XXXXXX***", así como al documento Word, que se adjuntaba, con sus nombres, apellidos y números de DNI/NIE o pasaporte, vulnerándose el principio de confidencialidad.
>
> Se entiende que las medidas de seguridad implantadas eran insuficientes, susceptibles de ser mejoradas; lo que se pone de manifiesto con la afirmación del Ayuntamiento de que ha procedido al REFORZAMIENTO de la política de seguridad.
>
> Es de resaltar que en el momento de tener conocimiento de la reclamación, desde el departamento de Protección de Datos se envió una Circular con las instrucciones a seguir a la hora de publicar listados que lleven aparejados datos personales, dirigida a todos los empleados del Ayuntamiento de Fuenlabrada, Organismos Autónomos y Empresas Municipales así como una segunda circular, también a todos los empleados, para recordar ciertos temas fundamentales relacionados con tratamientos en los que están implicados datos personales, asegurando que la información llega de manera inmediata a todos los interesados para que sea puesta en práctica y no se produzcan omisiones por desconocimiento en próximas actuaciones.
>
> En consecuencia, se DESESTIMARON las alegaciones.
>
> SEGUNDO. – ***(…).***
>
> El AYUNTAMIENTO, como responsable del tratamiento de datos, está obligado a aplicar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo que presente el tratamiento de datos.

Dichas medidas no solo son medidas de los sistemas informáticos sino también medidas de organizativas de factor humano.

El artículo 32 del RGPD no establece un listado delas medidas de seguridad que sean de aplicación de acuerdo con los datos que son objeto de tratamiento, sino que establece que el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas que sean adecuadas al riesgo que conlleve el tratamiento, teniendo en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, alcance, contexto y finalidades del tratamiento, los riesgos de probabilidad y gravedad para los derechos y libertades de las personas interesadas.

Asimismo, las medidas de seguridad deben resultar adecuadas y proporcionadas al riesgo detectado, señalando que la determinación de las medidas técnicas y organizativas deberá realizarse teniendo en cuenta: la seudonimización y el cifrado, la capacidad para garantizar la confidencialidad, integridad, disponibilidad y resiliencia, la capacidad para restaurar la disponibilidad y acceso a datos tras un incidente, proceso de verificación (que no auditoría), evaluación y valoración de la eficacia de las medidas.

En cualquier caso, de entre las medidas que se citan con relación al sistema de implantación del tratamiento de datos debemos destacar la obligatoriedad de las mismas en cumplimiento de la normativa vigente en materia de protección de datos.

En consecuencia, se DESESTIMARON las alegaciones.

TERCERO. – ***(…).***

Aun no tratándose de la publicación de un acto administrativo en los términos previstos en el artículo 45 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común, sí podemos afirmar que los receptores de dicho correo electrónico como participantes del programa “Banco del ***XXXXXX***”, formaban parte de un grupo de usuarios que voluntariamente se habían inscrito; si bien, en ningún momento, dieron su consentimiento para compartir la información difundida en dicho correo electrónico.

En ningún caso, el hecho de que no se trate de un trámite administrativo ni la urgencia ni la prisa justifican un acceso no autorizado a la información difundida a través de un correo electrónico.

Si existía el riesgo de que los empleados públicos envíen correos a los administrados sin copia oculta no se había tomado por el Ayuntamiento ninguna medida técnica de advertencia con el objeto de que el envío de dichos correos electrónicos cumpla con el principio de confidencialidad legalmente exigido. De entre las medidas aportadas, no había ninguna que mencionase este riesgo y las medidas a implantar.

En consecuencia, únicamente podríamos hablar de un error humano, puntual e independiente si existiendo dicha medida técnica de advertencia se hubiera enviado el correo electrónico sin copia oculta.

En consecuencia, se DESESTIMARON las alegaciones.

SÉPTIMO: Con fecha 8 de abril de 2022 se formuló propuesta de resolución, proponiendo:

IMPONER al AYUNTAMIENTO DE FUENLABRADA, con NIF P2805800F, por una infracción del Artículo 32 del RGPD, tipificada en el Artículo 83.4 del RGPD, una sanción de apercibimiento.

IMPONER al AYUNTAMIENTO DE FUENLABRADA, con NIF P2805800F, por una infracción del Artículo 5.1 f) del RGPD, tipificada en el Artículo 83.5 del RGPD, una sanción de apercibimiento.

IMPONER al AYUNTAMIENTO DE FUENLABRADA, con NIF P2805800F, por una infracción del Artículo 33 del RGPD, tipificada en el Artículo 83.4 del RGPD, una sanción de apercibimiento.

OCTAVO: Se acompañó a la propuesta de resolución como anexo relación de documentos obrantes en el procedimiento.

NOVENO: Notificada la propuesta de resolución y transcurrido el plazo para ello, no consta que se hayan presentado nuevas alegaciones por parte del AYUNTAMIENTO.

A la vista de todo lo actuado, por parte de la Agencia Española de Protección de Datos en el presente procedimiento se consideran hechos probados los siguientes,

HECHOS PROBADOS

PRIMERO: Consta acreditado que el AYUNTAMIENTO ha difundido datos personales de la parte reclamante sin su consentimiento.

SEGUNDO: Consta acreditado que el AYUNTAMIENTO ha enviado un correo electrónico “sin copia oculta” a una pluralidad de personas inscritas en la “lista Municipal del ***XXXXXX***”, así como que en dicho correo electrónico se adjuntaba un documento que incluía un listado con los datos personales (nombre, apellidos, y DNI) de estas personas.

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 y 48.1 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
Artículo 5.1.f) del RGPD

El artículo 5.1.f) "Principios relativos al tratamiento" del RGPD establece:

"1. Los datos personales serán:
(…)

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»)."

En el presente caso, queda acreditado que se ha producido un acceso no autorizado a las direcciones de correo electrónico de todos los participantes en el programa "Banco del ***XXXXXX***", adjuntando, además, un documento Word con sus nombres, apellidos y números de DNI/NIE o pasaporte, vulnerándose el principio de confidencialidad; si bien, no consta que se haya producido ninguna utilización ulterior, por parte de terceros, de la información personal de ninguno de los afectados.

Se imputa por tal motivo a la parte reclamada la comisión de una infracción por vulneración del artículo 5.1.f RGPD.

En el presente caso, la brecha de seguridad debe ser calificada de confidencialidad, como consecuencia del acceso no autorizado o ilícito a datos personales de la parte reclamante, debido al envío no autorizado de un escrito por parte de la parte reclamada.

Los datos de la parte reclamante han sido expuestos sin que se hayan adoptado las medidas previas necesarias para evitarlo, no estando amparada, según los actuales criterios de este organismo, su difusión, por lo que se considera acreditada la infracción descrita.

III
Tipificación de la infracción del artículo 5.1.f) del RGPD

La infracción del artículo 5.1.f) del RGPD se encuentra tipificada en el artículo 83.5 del RGPD que bajo la rúbrica "Condiciones generales para la imposición de multas administrativas" dispone:

“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:

a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9; (…)”

A este respecto, la LOPDGDD, en su artículo 71 “Infracciones” establece que “Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica”.

A efectos del plazo de prescripción, el artículo 72 “Infracciones consideradas muy graves” de la LOPDGDD indica:
“1. 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:

a) El tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 del Reglamento (UE) 2016/679. (…)”

IV
El Artículo 32 del RGPD establece:

“Seguridad del tratamiento

1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:
a) la seudonimización y el cifrado de datos personales;
b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
c)la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
d)un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros".

Se considera que la parte reclamada ha incumplido lo dispuesto en el artículo 32 del RGPD, al no contar con las medidas organizativas y técnicas apropiadas para impedir la exposición de datos personales.

A este respecto el AYUNTAMIENTO no ha aportado el análisis del riesgo relativo al envío de correos sin copia oculta ni la existencia de medidas específicas tendentes a evitar el envío a múltiples destinatarios sin usar la funcionalidad "con copia oculta".

V

Tipificación de la infracción del artículo 32 del RGPD

La infracción del artículo 32 del RGPD se encuentra tipificada en el artículo 83.4 del RGPD que bajo la rúbrica "*Condiciones generales para la imposición de multas administrativas*" dispone:

"Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

> *a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43; (…)"*

A este respecto, la LOPDGDD, en su artículo 71 *"Infracciones*" establece que *"Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica*".

A efectos del plazo de prescripción, el artículo 73 "*Infracciones consideradas graves*" de la LOPDGDD indica:

"En función de lo que establece el artículo 83.4 del Reglamento (UE) 2016/679 se consideran graves y prescribirán a los dos años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

> *(…)*
>
> *f) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al*

riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679.

VI

El Artículo 33 del RGPD establece:

El Artículo 33 "*Notificación de una violación de la seguridad de los datos personales a la autoridad de control*" del RGPD establece:

"1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

3. La notificación contemplada en el apartado 1 deberá, como mínimo:

a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;

b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;

c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;

d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo."

En el presente caso, consta que el AYUNTAMIENTO sufrió una brecha de seguridad de los datos personales en fecha 20 de noviembre del 2020; si bien, el AYUNTAMIENTO no fue consciente de la brecha de seguridad producida hasta el día 15 de febrero del 2021, cuando recibe a través del Registro de entrada del AYUNTAMIENTO el escrito de traslado de la reclamación que ha sido interpuesta en la AEPD.

En consecuencia, el AYUNTAMIENTO procedió a la notificación de la brecha de seguridad a la AEPD, el 17 de febrero de ese mismo año, en el plazo establecido en el RGPD a tal efecto y con las informaciones establecidas en el artículo 33 del RGPD.

Por ello, se considera que no existe infracción del artículo 33 del RGPD.

VII

El Artículo 83 "*Condiciones generales para la imposición de multas administrativas*" del RGPD apartado 7 establece:

"Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58, apartado 2, cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro."

Asimismo, el artículo 77 "*Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento*" de la LOPDGDD dispone lo siguiente:

"1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados...

> *c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local…*

2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución sancionando a las mismas con apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido.
(…)

5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo. (…)"

VIII

En el texto de la resolución se establecen cuáles han sido las infracciones cometidas y los hechos que han dado lugar a la vulneración de la normativa de protección de datos, de lo que se infiere con claridad cuáles son las medidas a adoptar, sin perjuicio de que el tipo de procedimientos, mecanismos o instrumentos concretos para implementarlas corresponda a la parte sancionada, pues es el responsable del tratamiento quien conoce plenamente su organización y ha de decidir, en base a la responsabilidad proactiva y en enfoque de riesgos, cómo cumplir con el RGPD y la LOPDGDD.

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 al AYUNTAMIENTO DE FUENLABRADA, con NIF P2805800F, por una infracción del Artículo 32 del RGPD, tipificada en el Artículo 83.4 del RGPD, una sanción de apercibimiento.

IMPONER al AYUNTAMIENTO DE FUENLABRADA, con NIF P2805800F, por una infracción del Artículo 5.1 f) del RGPD, tipificada en el Artículo 83.5 del RGPD, una sanción de apercibimiento.

SEGUNDO: PROCEDER AL ARCHIVO de las presentes actuaciones respecto a la infracción del artículo 33 RGPD.

TERCERO: NOTIFICAR la presente resolución al AYUNTAMIENTO DE FUENLABRADA.

CUARTO: COMUNICAR la presente resolución al Defensor del Pueblo, de conformidad con lo establecido en el artículo 77.5 de la LOPDGDD.

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.

938-050522

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