- Procedimiento Nº: PS/00144/2021

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: Don ***A.A.A.*** (en adelante, el reclamante), con fecha 18 de diciembre de 2019, interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra el AYUNTAMIENTO DE ******AYUNTAMIENTO.1*** con CIF P3502000G (en adelante, el reclamado).

Los motivos en que basa su reclamación son, en síntesis: que presentó una demanda de reclamación de cantidad contra el reclamado y señala que, una trabajadora de éste, ha enviado mediante WhatsApp a varios trabajadores la sentencia del citado procedimiento judicial en el que constan sus datos de carácter personal. Se aporta impresión de pantalla del terminal móvil con un mensaje de WhatsApp en el que se informa de la distribución de la sentencia.

SEGUNDO: De conformidad con 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 dio traslado, en fecha 18 de febrero de 2020, de dicha reclamación al reclamado, 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.

La solicitud de información fue entregada en fecha 24 de febrero de 2020, sin que se recibiese contestación.

TERCERO: Con fecha 6 de agosto de 2020, la Directora de la Agencia Española de Protección de Datos acordó admitir, formalmente, a trámite la reclamación presentada por el reclamante, de conformidad con el artículo 65 de la LOPDGDD.

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 reclamación, teniendo conocimiento de los siguientes extremos:

- Notificada al reclamado, con fecha de 11 de septiembre de 2020, solicitud de información sobre los hechos reclamados y la legitimación de acceso a este tipo de documentos por la persona que envió el mensaje de WhatsApp con el documento de la sentencia, transcurridos cuatro meses no se ha recibido en esta Agencia escrito de alegaciones remitido por el reclamado.

- Reiterada esta solicitud, con fecha de notificación de 25 de enero de 2021, no se ha recibido contestación del reclamado.

QUINTO: Con fecha 16 de abril de 2021, la Directora de la Agencia Española de

Protección de Datos acordó iniciar procedimiento sancionador al reclamado, por la presunta infracción del Artículo 32 del RGPD, Artículo 5.1.f) del RGPD, tipificada en el Artículo 83.5 del RGPD.

SEXTO: El acuerdo de inicio fue notificado electrónicamente al reclamado. Así lo exige el artículo 14.2 de la Ley 39/2015 de Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP) conforme al cual *"En todo caso estarán obligados a relacionarse a través de medios electrónicos con las Administraciones Públicas para la realización de cualquier trámite de un procedimiento administrativo, al menos, los siguientes sujetos: a) Las personas jurídicas".*

Obra en el expediente el Certificado emitido por el Servicio de Notificaciones Electrónicas y de Dirección Electrónica Habilitada de la FNMT-RCM, que deja constancia del envío del acuerdo de inicio, notificación de la AEPD dirigida al reclamado, a través de ese medio siendo la fecha de puesta a disposición en la sede electrónica del organismo el 16 de abril de 2021 y la fecha de rechazo automático el 27 de abril de 2021.

SÉPTIMO: De conformidad con el artículo 73.1 de la LPCAP el plazo para formular alegaciones al Acuerdo de Inicio es de diez días computados a partir del siguiente al de la notificación.

El artículo 64.2. LPACAP, indica que se informará al denunciado del derecho a formular alegaciones, del "*derecho a la audiencia en el procedimiento y de los plazos para su ejercicio, así como la indicación de que en caso de no efectuar alegaciones en el plazo previsto sobre el contenido del acuerdo de iniciación éste podrá ser considerado propuesta de resolución cuando contenga un pronunciamiento preciso acerca de la responsabilidad imputada".* (El subrayado es de la AEPD)

El acuerdo de inicio del expediente sancionador que nos ocupa contenía un pronunciamiento preciso sobre la responsabilidad de la entidad reclamada: en el citado acuerdo se concretaba cuál era conducta infractora, el tipo sancionador en el que era subsumible, las circunstancias de la responsabilidad descritas y la sanción que a juicio de la AEPD procedía imponer.

En consideración a lo expuesto y de conformidad con lo establecido en el artículo 64.2.f) de la LPACAP, el acuerdo de inicio del PS/00106/2021 es considerado Propuesta de Resolución: Notificado el acuerdo de inicio, el reclamado al tiempo de la presente resolución no ha presentado escrito de alegaciones, por lo que es de aplicación lo señalado en el artículo 64 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, que en su apartado f) establece que en caso de no efectuar alegaciones en el plazo previsto sobre el contenido del acuerdo de iniciación, éste podrá ser considerado propuesta de resolución cuando contenga un pronunciamiento preciso acerca de la responsabilidad imputada, por lo que se procede a dictar Resolución.

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

PRIMERO: Don ***A.A.A.,*** empleado público en excedencia del AYUNTAMIENTO DE ******AYUNTAMIENTO.1*** presentó una reclamación de cantidad a ese Ayuntamiento.

SEGUNDO: Dictada Sentencia sobre el asunto, una trabajadora del Ayuntamiento envió la Sentencia mediante WhatsApp a varios trabajadores. En la Sentencia constan datos de carácter personal del reclamante.

TERCERO: Se acompaña imagen de una pantalla de un teléfono móvil en el que una persona le indica al reclamado que ha recibido la Sentencia referida.

CUARTO: El Ayuntamiento reclamado no ha contestado a los requerimientos de información enviados por la Inspección de Datos de la Agencia Española de Protección de Datos relativos a esta reclamación, a pesar de haber recibido la notificación electrónica solicitando información en fechas 24 de enero y 11 de septiembre de 2020, y 25 de enero de 2021. El acuerdo de inicio notificado de la misma manera que los requerimientos de información, y, sin embargo, resultó expirada.

FUNDAMENTOS DE DERECHO

I

En virtud de los poderes que el artículo 58.2 del RGPD reconoce a cada autoridad de control, y según lo establecido en los arts. 47 y 48.1 de la LOPDGDD, la Directora de la Agencia Española de Protección de Datos es competente para resolver este procedimiento.

FUNDAMENTOS DE DERECHO

I

En virtud de los poderes que el artículo 58.2 del Reglamento 2016/679 (UE) de protección de datos (en adelante RGPD) reconoce 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 y Garantías de los derechos digitales (LOPDGDD), la Directora de la Agencia Española de Protección de Datos es competente para resolver este procedimiento.

II

Los hechos reclamados se concretan en una trabajadora del reclamado envió a través de la red social WhatsApp a varios trabajadores del consistorio la sentencia del procedimiento judicial instado por el reclamante contra el reclamado en el que constan sus datos de carácter personal.

El RGPD se ocupa en su artículo 5 de los principios que han de presidir el tratamiento de los datos personales y menciona entre ellos los de "*integridad y confidencialidad".* El precepto dispone:

"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, contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas (<<integridad y confidencialidad>>)".

El artículo 5.2. RGPD establece: "*El responsable del tratamiento será responsable del cumplimiento de los dispuesto en el apartado 1 y capaz de demostrarlo (<<responsabilidad proactiva>>)"*

El artículo 5, *Deber de confidencialidad*, de la nueva Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD), señala que:

"1. Los responsables y encargados del tratamiento de datos así como todas las personas que intervengan en cualquier fase de este estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1.f) del Reglamento (UE) 2016/679.

2. La obligación general señalada en el apartado anterior será complementaria de los deberes de secreto profesional de conformidad con su normativa aplicable.

3. Las obligaciones establecidas en los apartados anteriores se mantendrán aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento".

III

La documentación obrante en el expediente, y que no ha sido desvirtuada por el reclamado, acredita de que el reclamado, vulneró el artículo 5 del RGPD, principios relativos al tratamiento, en relación con el artículo 5 de la LOPGDD, deber de confidencialidad, al permitir que los datos de carácter personal del reclamante contenidos en sentencia judicial fueran publicados, a través de la red social WhatsApp, por una trabajadora del consistorio remitiéndose a otros trabajadores vulnerando el deber de confidencialidad.

Este deber de confidencialidad, con anterioridad deber de secreto, debe entenderse que tiene como finalidad evitar que se realicen filtraciones de los datos no consentidas por los titulares de los mismos.

Por tanto, ese deber de confidencialidad es una obligación que incumbe no sólo al responsable y encargado del tratamiento sino a todo aquel que intervenga en cualquier fase del tratamiento y complementaria del deber de secreto profesional.

IV

El artículo 83.5 a) del RGPD, considera que la infracción de *"los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9*" es sancionable, de acuerdo con el apartado 5 del mencionado artículo 83 del citado RGPD, "con multas administrativas de 20.000.000€ 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".

Por otro lado, la LOPDGDD, a efectos de prescripción, en su artículo 72 indica: *"Infracciones consideradas muy graves:*

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.
(…)"

V

El principio de integridad establecido en el artículo 5.1.f) RGPD se desarrolla a través de los artículos 32 a 34 RGPD, encuadrados en la sección II del capítulo IV que lleva por rúbrica "*Seguridad de los datos personales".* El artículo 32, "*Seguridad del tratamiento*", dice:

"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. (…)

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." (El subrayado es de la AEPD)

VI

La vulneración del artículo 32 del RGPD se encuentra tipificada en el artículo 83.4.a) del citado RGPD en los siguientes términos:

"4. 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.
(…)"

Por su parte, la LOPDGDD en su artículo 71, *Infracciones*, señala 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".*

Y en su artículo 73, a efectos de prescripción, califica de *"Infracciones consideradas graves":*

"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:

(…)
g) El quebrantamiento, como consecuencia de la falta de la debida diligencia, de las medidas técnicas y organizativas que se hubiesen implantado conforme a lo exigido por el artículo 32.1 del Reglamento (UE) 2016/679".
(…)"

VII

El RGPD define las violaciones de seguridad de los datos personales como *"todas aquellas violaciones de la seguridad que ocasionen la destrucción, perdida o alteración accidental o ilícita de datos personales trasmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos".*

De la documentación obrante en el expediente se constata que el reclamado, a través de una empleada de su organización, ha vulnerado el artículo 32 del RGPD, al producirse un incidente de seguridad en su sistema permitiendo el acceso a terceros de datos personales de otro empleado público, al ser exhibidos a través de la red social WhatsApp cuando una trabajadora remitió a otros trabajadores del consistorio sentencia judicial instada por el reclamante contra el consistorio permitiendo el acceso a sus datos de carácter personal con vulneración de las medidas de carácter técnico y

organizativas.

Hay que señalar que el RGPD en el citado precepto no establece un listado de las 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 todo caso, al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, 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 y que pudieran ocasionar daños y perjuicios físicos, materiales o inmateriales.

En este mismo sentido el considerando 83 del RGPD señala que:

"(83) A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como 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, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales".

La responsabilidad del reclamado viene determinada por la quiebra de seguridad puesta de manifiesto por el reclamante, ya que es responsable de tomar decisiones destinadas a implementar de manera efectiva las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo para asegurar la confidencialidad de los datos, restaurando su disponibilidad e impedir el acceso a los mismos en caso de incidente físico o técnico. Sin embargo, la entidad no solo ha incumplido esta obligación, sino que además traslada la reclamación para que informara a esta Agencia sobre la incidencia producida y comunicara sobre la decisión adoptada al respecto, hizo caso omiso no respondiendo nada.

De conformidad con lo que antecede, se estima que el reclamado es responsable de la infracción del RGPD: la vulneración del artículo 32, infracción tipificada en su artículo 83.4.a).

Sobre el plazo de prescripción de esta infracción, habremos de estar a las previsiones de la (LOPDGDD). El artículo 73, f) LOPDGDD califica de infracción grave "*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".* El artículo 73 LOPDGDD dispone que las infracciones graves tendrán un plazo de prescripción de dos años.

VIII

El artículo 83.7 del RGPD incida lo siguiente:

"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."

El ordenamiento jurídico español ha optado por no sancionar con multa a las entidades públicas, tal como se indica en el artículo 77 de la LOPDDGG, que establece lo siguiente:

"1. El régimen establecido en este artículo se aplicará a los tratamientos de los que sean responsables o encargados:

a) Los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos.
b) Los órganos jurisdiccionales.
c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.
d) Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas.
e) Las autoridades administrativas independientes.
f) El Banco de España.
g) Las corporaciones de Derecho público cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público.
h) Las fundaciones del sector público.
i) Las Universidades Públicas.
j) Los consorcios.
k) Los grupos parlamentarios de las Cortes Generales y las Asambleas Legislativas autonómicas, así como los grupos políticos de las Corporaciones Locales.

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 efec-

tos de la infracción que se hubiese cometido.

La resolución se notificará al responsable o encargado del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de interesado, en su caso.

3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.

Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda.

4. Se deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

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.

6. Cuando la autoridad competente sea la Agencia Española de Protección de Datos, esta publicará en su página web con la debida separación las resoluciones referidas a las entidades del apartado 1 de este artículo, con expresa indicación de la identidad del responsable o encargado del tratamiento que hubiera cometido la infracción.

Cuando la competencia corresponda a una autoridad autonómica de protección de datos se estará, en cuanto a la publicidad de estas resoluciones, a lo que disponga su normativa específica".

En el supuesto presente, ha quedado acreditado que la conducta referida constituye, por parte del reclamado la infracción a lo dispuesto en el artículo 5.1.f) y 32.1 del RGPD.

Asimismo, se establecerán las medidas que proceda adoptar para que cese la conducta, se corrijan los efectos de la infracción que se hubiese cometido y su adecuación a las exigencias contempladas en los artículos 5.1.f) y 32.1 del RGPD, así como la aportación de medios acreditativos del cumplimiento de lo requerido.

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 ***AYUNTAMIENTO.1** con CIF P3502000G, por una infracción del artículo 5.1.f) del RGPD, de conformidad con el artículo 83.5 a) del RGPD, una sanción de apercibimiento.

SEGUNDO: IMPONER al AYUNTAMIENTO DE ***AYUNTAMIENTO.1** con CIF P3502000G, por una infracción del artículo 32 del RGPD, de conformidad con el artículo 83.5 b) del RGPD, una sanción de apercibimiento.

TERCERO: De conformidad con el artículo 58.2. d) del RGPD, se ordena al responsable del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, debiendo informar a esta AEPD de su ejecución en el plazo de un mes.

CUARTO: NOTIFICAR la presente resolución al AYUNTAMIENTO DE ***AYUNTAMIENTO.1**.

QUINTO: 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.

938-131120

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