- **Procedimiento Nº: PS/00007/2021**

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, el reclamante) con fecha 31 de agosto de 2018 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra Gestión y Administración de Recibos S.A**.** con CIF A83052621 (en adelante, el reclamado).

Los motivos en que basa la reclamación son que el 30 de agosto de 2018 se recibe en varios buzones de correo electrónico, incluso en buzones de otra compañía, un correo procedente de "******EMAIL.1***" dirigido al reclamante para que se ponga en contacto con BBVA en relación con una financiación que mantiene con esa entidad.

El reclamante añade que la dirección de contacto que facilitó a BBVA no es la dirección corporativa de MAPFRE sino la personal de GMAIL.

Aporta la siguiente documentación:

- Correo electrónico procedente de ***"***EMAIL.1***" dirigido a la dirección de correo "******EMAIL.2***" y poniendo en copia las direcciones "******EMAIL.3***" y "******EMAIL.4***".

SEGUNDO: A la vista de los hechos denunciados en la reclamación y de los documentos aportados por el reclamante y de los hechos y documentos de los que ha tenido conocimiento esta Agencia, la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de los poderes de investigación otorgados a las autoridades de control en el artículo 57.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD).

Como resultado de las actuaciones de investigación practicadas, se constata que el responsable del tratamiento es el reclamado.

Asimismo, se constatan los siguientes extremos:

Con fecha 21 de noviembre de 2019, en el procedimiento E/06909/2018 la Agencia Española de Protección de Datos acordó llevar a cabo las actuaciones de investigación desarrolladas en el expediente E/00730/2019 en relación con los hechos reclamados.

Durante estas actuaciones se constató que el reclamante si había proporcionado la dirección corporativa de Mapfre a BBVA. Igualmente, se concluyó que el reclamado remitió el correo electrónico reclamado a buzones de correo ajenos al reclamante.

Transcurridos doce meses sin que se hayan podido concluir las actuaciones necesarias para esclarecer las posibles responsabilidades de los hechos reclamados, con fecha 3 de diciembre de 2019, en el procedimiento E/00730/2019 la Agencia Española de Protección de Datos acordó proceder al archivo de las actuaciones y abrir las presentes actuaciones de investigación, adscritas al expediente E/11745/2019.

Solicitado a BBVA el contrato específico de servicio mantenido con OPPLUS, con fecha de 8 de julio de 2020 se recibe en esta Agencia, con número de registro 023874/2020, el contrato de prestación de servicio requerido remitido por esta entidad.

Solicitada información a la entidad MAPFRE sobre las causas que motivaron el error de entrega al reclamante del correo remitido desde "…***EMAIL.1" e información y finalidad de los buzones "***EMAIL.5" y "***EMAIL.4", perteneciente este último a otra empresa, a donde se solicita que se envíe copia del mensaje en caso de error, con fecha de 8 de julio de 2020 se recibe en esta Agencia, con número de registro 023956/2020, escrito de alegaciones manifestando que el reclamante no guarda relación alguna con esta entidad e instando a esta Agencia a dirigir el requerimiento de información a la entidad MAPFRE TECH, por ser ésta, posiblemente, la entidad responsable del tratamiento de los datos del reclamante en los hechos a que se refiere su reclamación.

Solicitada la misma información indicada en el párrafo anterior a la entidad MAPFRE TECH, con fecha de 22 de octubre de 2020 se recibe en esta Agencia, con número de registro ***REGISTRO.1, escrito de alegaciones remitido por esta entidad manifestando los siguientes aspectos:

- Con respecto al error de entrega del correo remitido por "garsa.opplus.bbva.com" que desencadenó los hechos reclamados, este fue debido a la transferencia, con fecha de 1 de abril de 2018, por MAPFRE TECH a IBM GLOBAL SERVICES ESPANA, S.A. (en adelante, IBM GSE) de la unidad productiva en la que el reclamante prestaba sus servicios, por lo que el reclamante dejó de ser empleado de MAPFRE TECH pasando a ser empleado de IBM GSE, manteniendo sus derechos y obligaciones laborales en los términos regulados legalmente. Siendo ya empleado externo de MAPFRE, se le asigno una nueva cuenta de correo electrónico (…***EMAIL.6) con el dominio designado para el personal externo de otras compañías que prestan servicios a MAPFRE, programando en su antiguo buzón de correo el mensaje de error de entrega recibido por GYAR. Añaden en este punto que el correo facilitado por MAPFRE a sus empleados es para uso exclusivamente profesional tal y como expresamente se indica en la cláusula informativa de acceso a sus sistemas informáticos que todo usuario debe aceptar para poder continuar con el proceso de arranque del sistema:

> *"Está usted accediendo a un Sistema de Tratamiento de la Información propiedad de MAPFRE. El acceso y uso de este sistema está permitido exclusivamente a las personas autorizadas y para fines estrictamente profesionales."*

Como en la cláusula de confidencialidad que establece la obligación de los empleados respecto a esta materia que fue aceptada por el reclamante:

> *"Los recursos informáticos. tales como correo electrónico e Internet. son una herramienta de trabajo facilitada por el Grupo MAPFRE a sus empleados, por lo*

que su uso estará limitado a las funciones asociadas al desarrollo de la actividad profesional del usuario, quedando enterado el empleado de la prohibición de utilizar los mismos con fines particulares o ajenos al desempeño de su actividad laboral, pudiendo la empresa realizar cuantos actos de investigación, registro […]"

- Respecto a la función del buzón "******EMAIL.5***" manifiestan que se trata de un buzón interno de MAPFRE TECH creado para la correcta transición de MAPFRE TECH a IBM GSE de los servicios objeto del contrato de externalización para garantizar que no hubiese peticiones de servicio sin atender. Añaden que desconocen el motivo por el que BBVA remitió un mensaje a este buzón pese a que en el correo devuelto de error de entrega se identifica expresamente que se trata de un buzón de servicio. Finalmente indican que a este buzón tienen acceso seis empleados de MAPFRE TECH encargados de la supervisión y control de la adecuada transición de los servicios de externalización de MAPFRE a IBM GSE.

- Respecto a la función del buzón "******EMAIL.4***" se trata de un buzón operativo de IBM GSE con la misma función y finalidad que en el caso anterior pero gestionado por la empresa receptora de la externalización que igualmente se identifica expresamente en el correo devuelto de error de entrega, que se trata de un buzón de servicio. Añaden que a este buzón tienen acceso diez empleados de IBM GSE encargados de la supervisión y control de la adecuada transición de los servicios de externalización.

La manifestación realizada por el reclamante de que la dirección de correo facilitada a BBVA es únicamente la correspondiente a "gmail.com" no es correcta como se demostró en el seno del expediente E/00730/2019.

La utilización de los medios informáticos facilitados por Mapfre fueron aceptados por el reclamante como de único uso profesional, quedando por tanto excluida la función de la dirección de correo de Mapfre como medio de contacto para otros fines.

La manifestación realizada por el reclamante de que el correo indicado en la reclamación había sido difundido a unas tres mil personas, no es correcta. Se ha comprobado en las presentes actuaciones de investigación que a este correo tuvieron acceso seis personas de Mapfre Tech con funciones operativas y diez personas de IBM GSE con guales funciones.

La entidad GYAR, subencargada del tratamiento contratada por OPPLUS, realizó el envío del correo electrónico sobre la situación financiera del reclamante a buzones que claramente no correspondían al reclamante.

A partir del correo electrónico que ha motivado la reclamación, y que aporta el reclamante, se comprueba que una de las empleadas de IBM GSE con acceso al buzón de servicio "******EMAIL.4***", no reenvió el correo electrónico personal al reclamante, sino a una tercera persona de MAPFRE TECH.

TERCERO: Con fecha 25 de enero de 2021, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la reclamada, por las presuntas infracciones de los artículos 5.1 f) y 32 del RGPD, tipificadas en los artículos 83.5 a) y 83.4 a) del RGPD respectivamente.

CUARTO: 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.

QUINTO: De las actuaciones practicadas en el presente procedimiento, han quedado acreditados los siguientes:

HECHOS PROBADOS

PRIMERO: Consta que el 30 de agosto de 2018 se recibe en varios buzones de correo electrónico, incluso en buzones de otra compañía, un correo procedente de "***EMAIL.1*" dirigido al reclamante para que se ponga en contacto con BBVA en relación con una financiación que mantiene con esa entidad.

La dirección de contacto que facilitó el reclamante a BBVA no es la dirección corporativa de MAPFRE sino la personal de GMAIL.

- Correo electrónico procedente de "***EMAIL.1*" dirigido a la dirección de correo "***EMAIL.2*" y poniendo en copia las direcciones "***EMAIL.3*" y "***EMAIL.4*".

SEGUNDO: El reclamado, subencargado del tratamiento contratada por OPPLUS, realizó el envío del correo electrónico sobre la situación financiera del reclamante a buzones que claramente no correspondían al reclamante.

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.

II

La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, en su artículo 64 *"Acuerdo de iniciación en los procedimientos de naturaleza sancionadora"*, dispone:

"1. El acuerdo de iniciación se comunicará al instructor del procedimiento, con traslado de cuantas actuaciones existan al respecto, y se notificará a los interesados, entendiendo en todo caso por tal al inculpado.
Asimismo, la incoación se comunicará al denunciante cuando las normas reguladoras del procedimiento así lo prevean.

2. El acuerdo de iniciación deberá contener al menos:
a) Identificación de la persona o personas presuntamente responsables.

b) Los hechos que motivan la incoación del procedimiento, su posible calificación y las sanciones que pudieran corresponder, sin perjuicio de lo que resulte de la instrucción.
c) Identificación del instructor y, en su caso, secretario del procedimiento, con expresa indicación del régimen de recusación de los mismos.
d) Órgano competente para la resolución del procedimiento y norma que le atribuya tal competencia, indicando la posibilidad de que el presunto responsable pueda reconocer voluntariamente su responsabilidad, con los efectos previstos en el artículo 85.
e) Medidas de carácter provisional que se hayan acordado por el órgano competente para iniciar el procedimiento sancionador, sin perjuicio de las que se puedan adoptar durante el mismo de conformidad con el artículo 56.
f) Indicación del derecho a formular alegaciones y a la audiencia en el procedimiento y de los plazos para su ejercicio, así como 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.

3. Excepcionalmente, cuando en el momento de dictar el acuerdo de iniciación no existan elementos suficientes para la calificación inicial de los hechos que motivan la incoación del procedimiento, la citada calificación podrá realizarse en una fase posterior mediante la elaboración de un Pliego de cargos, que deberá ser notificado a los interesados".

En aplicación del anterior precepto y teniendo en cuenta que no se han formulado alegaciones al acuerdo de inicio, procede resolver el procedimiento iniciado.

III

Se imputa al reclamado la vulneración de los artículos 5.1 f) y 32 del RGPD.

El RGPD establece en el artículo 5 los principios que han de regir el tratamiento de los datos personales y menciona entre ellos el de *"integridad y confidencialidad".*

El artículo señala que:

"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»)".

A su vez, la seguridad de los datos personales viene regulado en el artículo 32 del RGPD.

El artículo 32 del RGPD *"Seguridad del tratamiento",* establece que:

"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".

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".

III

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 ofrecen indicios evidentes de que el reclamado ha vulnerado el artículo 32 del RGPD, al producirse una brecha de seguridad en sus sistemas dado que se recibe en varios buzones de correo electrónico, incluso en buzones de otra compañía, un correo procedente de "******EMAIL.1***" dirigido al reclamante para que se ponga en contacto con BBVA en relación con una financiación que mantiene con esa entidad.

Por tanto, no cabe duda, vista la legislación aplicable, la falta de medidas organizativas o técnicas establecidas por el reclamado, pudiendo haber determinado un protocolo que diga a los empleados que no pueden hacerlo o algún mecanismo en el propio correo electrónico que avise de que el email se está enviando a varios destinatarios antes de que se envíe, que impidan que se pierda la confidencialidad de los datos, lo que conlleva a su vez la infracción 5.1 f) del RGPD.

Hay que señalar que el RGPD su artículo 32 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".

IV

El artículo 72.1.a) de la LOPDGDD señala 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:*

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

No obstante, el artículo 58.2 del RGPD dispone lo siguiente: *"Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:*

(…)

b) sancionar a todo responsable o encargado del tratamiento con apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento;

(…)"

Por tanto, el RGPD, sin perjuicio de lo establecido en su artículo 83, contempla en su artículo 58.2 b) la posibilidad de acudir al apercibimiento para corregir los tratamientos de datos personales que no se adecúen a sus previsiones.

De conformidad con las evidencias de las que se dispone y de la documentación aportada se desprende que el reclamado realizó el envío del correo electrónico sobre la situación financiera del reclamante a buzones que claramente no correspondían al reclamante, vulnerando el deber de confidencialidad, lo cual constituye, por parte del reclamado, de dos infracciones, una contra lo dispuesto en el artículo 32 del RGPD y otra contra lo dispuesto en el artículo 5.1 f) del RGPD, que rige los principios de integridad y confidencialidad de los datos personales, así como la responsabilidad proactiva del responsable del tratamiento de demostrar su cumplimiento.

Estas infracciones son sancionadas con apercibimiento. De acuerdo con el artículo 58.2.b) del RGPD, y al considerar que las multas administrativas que pudieran recaer con arreglo a los dispuesto en el artículo 83.5.b) del RGPD constituiría una carga desproporcionada para el reclamado.

Asimismo, a los efectos previstos en el artículo 58.2 del RGPD la medida correctiva que podría imponerse al reclamado consistiría en requerirle que proceda a adoptar las medidas necesarias para que cese la conducta objeto de esta reclamación, que ha causado la brecha de seguridad denunciada, para que se corrijan los efectos de la infracción cometida y su adecuación a las exigencias contempladas en el artículo 32 del RGPD, así como la aportación de medios acreditativos del cumplimiento de lo requerido.

Por lo tanto, de acuerdo con la legislación aplicable, la Directora de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: IMPONER a Gestión y Administración de Recibos S.A**.** con CIF A83052621:

- por una infracción del artículo 32 del RGPD, tipificada en el artículo 83.4 a) del RGPD una sanción de apercibimiento y requerirle para que informe a la AEPD de las medidas adoptadas, en el plazo de un mes, para que se corrijan los efectos de la infracción cometida y su adecuación a las exigencias contempladas en el artículo 32 del RGPD.

- por una infracción del artículo 5.1 f) del RGPD, tipificada en el artículo 83.5 a) del RGPD una sanción de apercibimiento.

SEGUNDO: NOTIFICAR la presente resolución a Gestión y Administración de Recibos S.A**.** con CIF A83052621.

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.

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