Procedimiento nº: **PS/00243/2018**

ASUNTO: Recurso de Reposición Nº. RR/00734/2018

Examinado el recurso de reposición interpuesto por la entidad ***COMMCENTER, S.A.*** contra la resolución dictada por la Directora de la Agencia Española de Protección de Datos en el procedimiento sancionador PS/00243/2018, y en base a los siguientes

HECHOS

PRIMERO: Con fecha 3 de octubre de 2018, se dictó resolución por la Directora de la Agencia Española de Protección de Datos en el procedimiento sancionador, PS/00243/2018, en virtud de la cual se imponía a ***COMMCENTER, S.A.*** por infracción del artículo 9.1 de la LOPD, tipificada como grave en el artículo 44.3.h) de la misma Ley, una sanción de 40.001 € (cuarenta mil un euro), de conformidad con lo establecido en el artículo 45.2 de la citada LOPD.

Dicha resolución, que fue notificada al recurrente en fecha 04/10/2018, fue dictada previa la tramitación del correspondiente procedimiento sancionador, de conformidad con lo dispuesto en el artículo 127 del reglamento de desarrollo de la LOPD aprobado por el Real Decreto 1720/2007, de 21 de diciembre.

SEGUNDO: Como hechos probados del citado procedimiento sancionador, PS/00243/2018, quedó constancia de los siguientes:

PRIMERO. *El 13/02/2018 tiene entrada en la AEPD escrito del afectado denunciando la recepción en su cuenta de correo ***EMAIL.1 de contratos de financiación de productos con TELEFÓNICA CONSUMER, en los que figuran datos de carácter personal relativos a terceros, entre los que se encuentran funcionarios, autónomos, jubilados, etc.*

SEGUNDO. *Consta aportada copia del DNI del denunciante nº ***DNI.1.*

TERCERO. *El denunciante ha aportado copia de trece solicitudes de financiación de productos de distintos clientes con TELEFÓNICA CONSUMER, recibidos en su cuenta de correo ***EMAIL.1, en los que constan los datos personales de los solicitantes, el nombre del establecimiento en que se adquieren los productos (COMMCENTER), los datos económicos, las condiciones del préstamo, cuentas de domiciliación bancaria, firma de los solicitantes, etc.*

CUARTO. *El 14/03/2018 el denunciante ha aportado las cabeceras de todos los e-mails recibidos en la dirección de correo electrónico ***EMAIL.1.*

QUINTO. *EL denunciante en escrito de 24/07/2018 ha aportado nuevo e-mail de fecha 04/04/2018, con su cabecera correspondiente, recibido en su dirección de correo electrónico ***EMAIL.1 relativa a una nueva solicitud-contrato de financiación en establecimiento de COMMCENTER.*

SEXTO. *En el Acta de Inspección E/00800/0218/I-01 realizada por los Servicios de Inspección de esta Agencia en el establecimiento de COMMCENTER el 16/05/2018,*

se señala lo siguiente:

"1. Los inspectores comunican al representante de COMMCENTER que su visita tiene relación con la denuncia presentada en la Agencia Española de Protección de Datos.
2. El representante de COMMCENTER realiza las siguientes manifestaciones en respuesta a las cuestiones planteadas por los inspectores:
2.1 COMMCENTER es distribuidor oficial y exclusivo de MOVISTAR, entidad con la que tiene suscritos los correspondientes contratos para la realización de dichos servicios.
2.2. Los clientes que adquieren productos en la tienda tienen la opción de financiar su compra, financiación que se realiza a través de TELEFÓNICA CONSUMER FINANCE SAU, entidad con la que COMMCENTER ha suscrito los correspondientes contratos de prestación de servicios. Los inspectores de la Agencia solicitan al representante de COMMCENTER copia de dichos contratos, manifestando que los mismos se encuentran en los servicios centrales.
2.3. Para la realización de la operación financiera COMMCENTER dispone de una aplicación WEB facilitada por TELEFÓNICA CONSUMER FINANCE SAU, a través de la cual se gestionan las solicitudes. El acceso a dicha aplicación requiere la introducción de un código de usuario y una contraseña que es único para cada tienda y compartido por todos los empleados de la misma tienda.
3. Los inspectores de la Agencia realizan las siguientes comprobaciones:
3.1. Desde el puesto de trabajo de una de las empleadas se realiza el seguimiento de una simulación de una operación de financiación para la renovación de un terminal.
3.2. Se comprueba que para proceder a la realización de la operación la empleada escanea el documento de identidad del cliente, que se introduce en el sistema informático.
3.3. Posteriormente, se accede a la aplicación WEB denominada "CONSUMER FINANCE" la cual solicita la introducción de un código de establecimiento y una clave de acceso.
3.4. Se verifica que la aplicación solicita unos datos iniciales relativos al producto a financiar, posteriormente solicita la introducción de datos económicos y a continuación se solicitan datos personales del solicitante.
3.5. Se verifica que entre los datos personales solicitados se incluye la dirección de correo electrónico y que la introducción de dicho dato es obligatorio para poder continuar con la operación. El representante de COMMCENTER manifiesta que dicho campo es obligatorio para poder finalizar la operación, ya que es la dirección electrónica a la que se envía copia del contrato de financiación y las condiciones generales.
En respuesta a la pregunta de los inspectores, el representante de COMMCENTER manifiesta que cuando un cliente no tiene dirección de correo electrónico se le crea una nueva en el terminal que compra.
Se adjunta como documento número 1 impresiones de pantalla de las comprobaciones realizadas.
4. Los inspectores de la Agencia muestran al representante de COMMCENTER copia de 13 solicitudes de contrato en las que consta que han sido realizadas en el establecimiento en el que se lleva a cabo la presente inspección, que se adjuntan como documento número 2. El representante de COMMCENTER realiza las siguientes manifestaciones en respuesta a las preguntas formuladas por los inspectores:
4.1. Desconocen el motivo por el que en dichas solicitudes de financiación aparece la

*dirección de correo electrónico ***EMAIL.1. Cuando un cliente no dispone de dirección de correo electrónico y no desea una de nueva creación en el terminal adquirido, se le informa de que no es posible continuar con la operación.*
5. Los inspectores de la Agencia solicitan al representante de COMMCENTER confirmación de la realización de las operaciones que aparecen en los documentos mostrados. El representante del COMMCENTER accede al fichero de facturación de COMMCENTER, comprobando que aparecen facturadas en COMMCENTER todas las operaciones mostradas en el documento número 2 excepto una correspondiente al de 4 de diciembre, que según manifiesta el representante de COMMCENTER puede ser debido a que no se le aprobó la financiación.
Se adjunta como documento número 3 copia impresa de las facturas emitidas.
6. A requerimiento de los inspectores, el representante de COMMCENTER entrega copia del documento "MANUAL CONSUMER FINANCETCE", que se adjunta como documento número 4.
7. Los inspectores de la Agencia recaban la documentación mencionada, que se entrega voluntaria y libremente por el inspeccionado a requerimiento de los inspectores.
(…)

SEPTIMO. *COMMCENTER en escrito de 16/05/2018 ha aportado el contrato suscrito para la prestación del servicio de gestión de solicitudes de financiación que fue concertado el 10/11/2011 entre TELEFONICA MOVILES DE ESPAÑA, S.A. y FINCONSUM, EFC, S.A. Contiene cláusula OCTAVA relativa a Confidencialidad y Protección de Datos.*

OCTAVO. *COMMCENTER en escrito de 19/06/2018 reconoce que "A la vista de la denuncia e investigación llevada a cabo por parte de la AEPD todo apunta a que lo realmente acontecido es que, a la hora de rellenar en el formulario de solicitud de financiación de algunos clientes, una de sus trabajadoras, …, ha rellenado el campo de la dirección de email genéricamente con el correo electrónico ***EMAIL.1.*
Una cuenta que la trabajadora podría creer inexistente, al referirse a la provincia donde se encuentra sita la tienda desde la que operaba con la única intención de no ver bloqueado con el procedimiento de financiación pero que realmente pertenecía al denunciante sin que se tuviese constancia al respecto".

TERCERO: **COMMCENTER, S.A.** (en lo sucesivo el recurrente) ha presentado en fecha 05/11/2018, en esta Agencia Española de Protección de Datos, recurso de reposición fundamentándolo en vicio de nulidad de pleno derecho; la incorrecta consideración como responsable del tratamiento y la no tenencia en cuenta del cumplimiento de sus obligaciones en materia de protección de datos.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver el presente recurso la Directora de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto en el artículo 123 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo LPACAP).

II

En relación con las manifestaciones efectuadas por el recurrente, reiterándose básicamente en las alegaciones ya presentadas a lo largo del procedimiento sancionador, debe señalarse que todas ellas ya fueron analizadas y desestimadas en los Fundamentos de Derecho del II a V ambos inclusive, de la Resolución recurrida, tal como se transcribe a continuación:

II

Se imputa a la entidad COMMCENTER la vulneración del principio de seguridad de los datos personales, establecido en el artículo 9.1 de la LOPD.

El artículo 7 del Convenio Nº108 del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, establece:

"Seguridad de los datos:

Se tomarán medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados".

El Art 17.1 de la Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, establece:

"Seguridad del tratamiento:

1. Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales. Dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse"

Por otra parte, la LOPD, traspuso al ordenamiento interno el contenido de la Directiva 95/46. En el artículo 9 de la citada LOPD se dispone lo siguiente:

"1. El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten la alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley".

El citado artículo 9 de la LOPD establece el "principio de seguridad de los datos" imponiendo la obligación de adoptar las medidas de índole técnica y organizativa que garanticen dicha seguridad, añadiendo que tales medidas tienen como finalidad evitar, entre otros aspectos, el "acceso no autorizado" por parte de terceros.

Para poder delimitar cuáles sean los accesos que la Ley pretende evitar exigiendo las pertinentes medidas de seguridad es preciso acudir a las definiciones de "fichero" y "tratamiento" contenidas en la LOPD.

En lo que respecta al concepto de "fichero" el artículo 3.b) de la LOPD lo define como "todo conjunto organizado de datos de carácter personal", con independencia de la modalidad de acceso al mismo.

Por su parte el artículo 3.c) de la citada Ley Orgánica considera tratamiento de datos cualquier operación o procedimiento técnico que permita, en lo que se refiere al objeto del presente procedimiento, la "comunicación" o "consulta" de los datos personales tanto si las operaciones o procedimientos de acceso a los datos son automatizados o no.

Y el artículo 3.a) de dicha Ley añade que se entenderá por datos de carácter personal "cualquier información concerniente a personas físicas identificadas o identificables".

En este mismo sentido se pronuncia el artículo 2 a) de la Directiva 95/46/CE del Parlamento y del Consejo, de 24 de octubre de 1995, relativa a la Protección de las Personas Físicas en lo que respecta al tratamiento de datos profesionales y a la libre circulación de estos datos, que dispone "toda información sobre una persona física identificada o identificable (el «interesado»); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social".

Para completar el sistema de protección en lo que a la seguridad afecta, el artículo 44.3.h) de la LOPD tipifica como infracción grave el mantener los ficheros "...que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen".

Sintetizando las previsiones legales puede afirmarse que:

a) Las operaciones y procedimientos técnicos automatizados o no, que permitan el acceso, –la comunicación o consulta- de datos personales, es un tratamiento sometido a las exigencias de la LOPD.

b) Los ficheros que contengan un conjunto organizado de datos de carácter personal así como el acceso a los mismos, cualquiera que sea la forma o modalidad en que se produzca están, también, sujetos a la LOPD.

c) La LOPD impone al responsable del fichero la adopción de medidas de seguridad, cuyo detalle se remite a normas reglamentarias, que eviten accesos no autorizados.

d) El mantenimiento de ficheros carentes de medidas de seguridad que permitan accesos o tratamientos no autorizados, cualquiera que sea la forma o modalidad de éstos, constituye una infracción tipificada como grave.

Las medidas de seguridad se clasifican en atención a la naturaleza de la información tratada, esto es, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la misma. Dichas medidas, en el caso que nos ocupa, deben salvaguardar la confidencialidad y seguridad de los datos de carácter personal recabados por COMMCENTER, correspondiendo adoptar las calificadas de nivel básico, en atención al tipo de información básica que contiene, tal como se especifica en el artículo 80 del RD 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD.

Las medidas de seguridad de nivel básico están reguladas en los artículos 89 a 94, las de nivel medio se regulan en los artículos 95 a 100 y las medidas de seguridad de nivel alto se regulan en los artículos 101 a 104, del Reglamento de desarrollo de la LOPD.

El artículo 93 del citado Reglamento, aplicable a todos los ficheros y tratamientos automatizados, establece:

"Artículo 93. Identificación y autenticación.

1. El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.
2. El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.
3. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.
4. El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible".

También, el artículo 5.2.b) del Reglamento de desarrollo de la LOPD define la autenticación como el procedimiento de comprobación de la identidad de un usuario; el mismo artículo, letra h), define la identificación como el procedimiento de reconocimiento de la identidad de un usuario; corresponde al responsable del fichero o tratamiento comprobar la existencia de la autorización exigida en el citado artículo 91, con un proceso de verificación de la identidad de la persona (autenticación) implantando un mecanismo que permita acceder a datos o recursos en función de la identificación ya autenticada. Cada identidad personal deberá estar asociada con un perfil de seguridad, roles y permisos concedidos por el responsable del fichero o tratamiento.

En definitiva, COMMCENTER estaba obligada a adoptar, de manera efectiva, las medidas técnicas y organizativas previstas para los ficheros de la naturaleza indicada y, entre ellas, las dirigidas a impedir el acceso no autorizado por parte de terceros a los datos personales que constan en sus ficheros. En este caso, sin embargo, ha quedado acreditado que la citada entidad incumplió esta obligación, como lo acredita que las solicitudes de financiación y demás documentos fueran remitidos a la dirección de correo electrónico del denunciante, lo que demuestra que la aplicación implantada para la recogida de datos de carácter personal era defectuosa y no cumplía los requisitos técnicos y de seguridad requeridos.

Por tanto, el mecanismo contenido en los sistemas de la entidad, no cumplía las exigencias contenidas en los artículos antes reseñados sobre control de accesos, identificación y autenticación de usuarios, por cuanto que la aplicación web a través de la cual se gestionaban las solicitudes de financiación requería la introducción de una serie de datos, entre los que se incluía la dirección de correo electrónico, dato obligatorio para poder continuar con las operaciones ya que era la dirección electrónica a la que se enviaba la copia del contrato de financiación y las condiciones generales; sin embargo, dichos documentos fueron enviados a la dirección ******EMAIL.1*** *perteneciente al denunciante.*

Además, los propios representantes de la entidad a pregunta de los inspectores señalaron que cuando un cliente carecía de dirección de correo electrónico se le creaba una nueva en el terminal que compra ya que en caso contrario no era posible continuar con la operación de financiación.

*La representación de la entidad ha reconocido en escrito de 19/06/2018 que "A la vista de la denuncia e investigación llevada a cabo por parte de la AEPD todo apunta a que lo realmente acontecido es que, a la hora de rellenar en el formulario de solicitud de financiación de algunos clientes, una de sus trabajadoras, …, ha rellenado el campo de la dirección de email genéricamente con el correo electrónico ***EMAIL.1.*

Una cuenta que la trabajadora podría creer inexistente, al referirse a la provincia donde se encuentra sita la tienda desde la que operaba con la única intención de no ver bloqueado con el procedimiento de financiación pero que realmente pertenecía al denunciante sin que se tuviese constancia al respecto".

En consecuencia, se considera que la entidad COMMCENTER ha incurrido en la infracción grave descrita.

III

Por otra parte, en esta materia se impone una obligación de resultado, que conlleva la exigencia de que las medidas implantadas deben impedir, de forma efectiva, el acceso a la información por parte de terceros. Esta necesidad de especial diligencia en la custodia de la información por el responsable ha sido puesta de relieve por la Audiencia Nacional, en su Sentencia de 11/12/08 (recurso 36/08), fundamento cuarto: "Como ha dicho esta Sala en múltiples sentencias…se impone, en consecuencia, una obligación de resultado, consistente en que se adoptan las medidas necesarias para evitar que los datos se pierdan, extravíen o acaben en manos de terceros…la recurrente es, por disposición legal una deudora de seguridad en materia de datos, y por tanto debe dar una explicación adecuada y razonable de cómo los datos han ido a parar a un lugar en el que son susceptibles de recuperación por parte de terceros, siendo insuficiente con acreditar que adopta una serie de medidas, pues es también responsable de que las mismas se cumplan y se ejecuten con rigor".

Y en cuanto a la ausencia de culpabilidad alegada por la representación de la denunciada hay que señalar que el principio de culpabilidad es exigido en el procedimiento sancionador y así la STC 246/1991 considera inadmisible en el ámbito del Derecho administrativo sancionador una responsabilidad sin culpa. Pero el principio de culpa no implica que sólo pueda sancionarse una actuación intencionada y a este respecto el artículo 130.1 de la Ley 30/1992, de 26 de noviembre, de

Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, dispone "sólo podrán ser sancionadas por hechos constitutivos de infracción administrativa las personas físicas y jurídicas que resulten responsables de los mismos aun a título de simple inobservancia."

El Tribunal Supremo (STS 16 de abril de 1991 y STS 22 de abril de 1991) considera que del elemento culpabilista se desprende "que la acción u omisión, calificada de infracción sancionable administrativamente, ha de ser, en todo caso, imputable a su autor, por dolo o imprudencia, negligencia o ignorancia inexcusable". El mismo Tribunal razona que "no basta...para la exculpación frente a un comportamiento típicamente antijurídico la invocación de la ausencia de culpa" sino que es preciso "que se ha empleado la diligencia que era exigible por quien aduce su inexistencia." (STS 23 de enero de 1998).

Esta necesidad de especial diligencia en la custodia de la información por el responsable ha sido puesta de relieve por la Audiencia Nacional, en su Sentencia de 11/12/08 (recurso 36/08), fundamento cuarto: "Como ha dicho esta Sala en múltiples sentencias…se impone, en consecuencia, una obligación de resultado, consistente en que se adoptan las medidas necesarias para evitar que los datos se pierdan, extravíen o acaben en manos de terceros…la recurrente es, por disposición legal una deudora de seguridad en materia de datos, y por tanto debe dar una explicación adecuada y razonable de cómo los datos han ido a parar a un lugar en el que son susceptibles de recuperación por parte de terceros, siendo insuficiente con acreditar que adopta una serie de medidas, pues es también responsable de que las mismas se cumplan y se ejecuten con rigor".

*Por tanto, a la luz de lo señalado anteriormente la entidad ha adolecido de falta de diligencia como lo demuestra que los procedimientos y protocolos de actuación devinieran ineficaces e incongruentes y el que los propios representantes de la entidad desconocieran el motivo por el que las solicitudes de financiación se remitieran a la dirección de correo electrónico *****EMAIL.1** titularidad del denunciante y que se espera que con las nuevas medidas implantadas por la entidad lo acontecido no vuelva a suceder en el futuro.*

IV

El artículo 44.3.h) de la LOPD, considera infracción grave:

"Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen".

Dado que ha existido vulneración del "principio de seguridad de los datos", recogido en el artículo 9 de la LOPD, se considera que COMMCENTER ha incurrido en la infracción grave descrita.

V

El artículo 45.2, 4 y 5 de la LOPD establece que:

"2. Las infracciones graves serán sancionadas con multa de 40.001 € a 300.000 €

(…)

4. La cuantía de las sanciones se graduará atendiendo a los siguientes criterios:

a) El carácter continuado de la infracción.
b) El volumen de los tratamientos efectuados.
c) La vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal.
d) El volumen de negocio o actividad del infractor.
e) Los beneficios obtenidos como consecuencia de la comisión de la infracción.
f) El grado de intencionalidad.
g) La reincidencia por comisión de infracciones de la misma naturaleza.
h) La naturaleza de los perjuicios causados a las personas interesadas o a terceras personas.
i) La acreditación de que con anterioridad a los hechos constitutivos de infracción la entidad imputada tenía implantados procedimientos adecuados de actuación en la recogida y tratamiento de Ios datos de carácter personal, siendo la infracción consecuencia de una anomalía en el funcionamiento de dichos procedimientos no debida a una falta de diligencia exigible al infractor.
j) Cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.

5. El órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate, en los siguientes supuestos:

a) Cuando se aprecie una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho como consecuencia de la concurrencia significativa de varios de los criterios enunciados en el apartado 4 de este artículo.
b) Cuando la entidad infractora haya regularizado la situación irregular de forma diligente.
c) Cuando pueda apreciarse que la conducta del afectado ha podido inducir a la comisión de la infracción.
d) Cuando el infractor haya reconocido espontáneamente su culpabilidad.
e) Cuando se haya producido un proceso de fusión por absorción y la infracción fuese anterior a dicho proceso, no siendo imputable a la entidad absorbente".

COMMCENTER ha solicitado la exoneración de responsabilidad y subsidiariamente imposición de una sanción en grado mínimo, aplicando la escala relativa a la clase de infracciones que precede inmediatamente en gravedad a aquella en la que se integra la considerada en el presente caso, de conformidad con el artículo 45.5.d) de la LOPD.

Hay que señalar que el citado apartado 45.5 de la LOPD deriva del principio de proporcionalidad de la sanción y permite establecer "la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate", pero para ello

es necesario la concurrencia de, o bien una cualificada disminución de la culpabilidad del imputado, o bien de la antijuridicidad del hecho, o bien de alguna otra de las circunstancias que el mismo precepto cita.

En cuanto a la aplicación de lo dispuesto en el artículo 45.5 de la LOPD, la Sentencia de 21/01/2004 de la Audiencia Nacional, en su recurso 1939/2001, señaló que dicho precepto "…no es sino manifestación del llamado principio de proporcionalidad (artículo 131.1 de la LRJPAC), incluido en el más general de la prohibición de exceso, reconocido por la jurisprudencia como principio general del Derecho. Ahora bien, la presente regla debe aplicarse con exquisita ponderación y sólo en los casos en los que la culpabilidad y la antijuridicidad resulten sustancialmente atenuadas, atendidas las circunstancias del caso concreto. Lo cual insistimos puede darse, por excepción, en casos muy extremos (de aquí la expresión "especialmente cualificada") y concretos".

En el presente caso, tanto de las actuaciones practicadas como de la documentación aportada al expediente, ha quedado acreditado que COMMCENTER vulneró el artículo 9.1 de la LOPD, en relación con los artículos 93 del RLOPD, al no adoptar las medidas técnicas y organizativas necesarias previstas, entre ellas, la adopción de medidas específicamente destinadas a impedir el acceso no autorizado por parte de terceros a los datos personales de sus ficheros, como lo acredita que las solicitudes de financiación y demás documentos fueran remitidos a la dirección de correo electrónico del denunciante, demostrando que la aplicación implantada era defectuosa y no cumplía los requisitos técnicos y de seguridad requeridos, por lo que su actuación ha de ser objeto de sanción..

*La propia entidad, como consta en el hecho probado octavo, ha reconocido que "A la vista de la denuncia e investigación llevada a cabo por parte de la AEPD todo apunta a que lo realmente acontecido es que, a la hora de rellenar en el formulario de solicitud de financiación de algunos clientes, una de sus trabajadoras, …, ha rellenado el campo de la dirección de email genéricamente con el correo electrónico ***EMAIL.1.*

Una cuenta que la trabajadora podría creer inexistente, al referirse a la provincia donde se encuentra sita la tienda desde la que operaba con la única intención de no ver bloqueado con el procedimiento de financiación pero que realmente pertenecía al denunciante sin que se tuviese constancia al respecto".

Por tanto, no se dan las citadas circunstancias señaladas lo que impide apreciar la existencia de motivos para la aplicación de la facultad contemplada en el artículo 45.5, debido, por un lado, no obra en el expediente ningún elemento que lleve a apreciar la concurrencia de alguna de las circunstancias previstas en los apartados a) b), c), d) y e) del referido artículo y, por otro, a la especial diligencia y conocimiento de la normativa de protección de datos que se ha de exigir a las entidades profesionales cuando, como ocurre con la entidad imputada, el tratamiento de datos personales constituye parte habitual y esencial de su actividad. Las empresas que por su actividad están habituadas al tratamiento de datos personales deben ser especialmente diligentes y cuidadosas al realizar operaciones con ellos y deben optar siempre por la interpretación más favorable a la salvaguarda del derecho fundamental a la protección de datos (como de forma reiterada sostiene la Audiencia Nacional, entre otras en Sentencia de 26 de noviembre de 2008).

Por otra parte, en relación con los criterios de graduación de las sanciones que contempla el artículo 45.4 de la LOPD, se aprecia la concurrencia de las siguientes circunstancias agravantes:

- El apartado a) "El carácter continuado de la infracción", puesto que los datos de carácter personal que el denunciante fue recibiendo en su cuenta de correo tuvo lugar desde septiembre de 2017 hasta abril de 2018 (último correo aportado por el denunciante)

- El apartado b) "El volumen de los tratamientos efectuados", la información aportada acredita hasta 14 solicitudes de financiación remitida por la oficina de COMMCENTER al denunciante.

- El apartado c) "La vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal", ya que la actividad de la denunciada exige un tratamiento de datos de carácter personal tanto de clientes como de terceros.

- El apartado d) "El volumen de negocio o actividad del infractor", puesto que se trata de una gran empresa dentro de su sector de negocio o actividad.

En el presente caso, valorados los criterios de graduación de las sanciones establecidos en el artículo 45.4, tanto favorables como adversos, se impone una sanción de 40.001 € por la infracción del artículo 9.1 de la LOPD, en relación con el artículo 93 del RLOPD, de la que COMMCENTER debe responder.

III

La representación del recurrente en su escrito de recurso ha alegado que la resolución recurrida incurre en vicio de nulidad de pleno derecho por invalidez sobrevenida del artículo 45 LOPD; la incorrecta consideración como responsable del tratamiento y que se obvia el cumplimiento de sus obligaciones en base a la LOPD y su normativa de desarrollo.

El R.D. Ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos, en su *Disposición transitoria primera*, regula el régimen transitorio de los procedimientos, determinando que:

"1. Los procedimientos ya iniciados a la entrada en vigor de este real decreto-ley se regirán por la normativa anterior, salvo que el régimen establecido en el mismo contenga disposiciones más favorables para el interesado.

2. Lo dispuesto en el apartado anterior será asimismo de aplicación a los procedimientos respecto de los cuales ya se hubieren iniciado las actuaciones previas a las que se refiere la Sección 2.ª del Capítulo III del Título IX del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, aprobado por Real Decreto 1720/2007, de 21 de diciembre".

La *Disposición derogatoria única* del citato R.D. Ley señala que:

"Quedan derogadas todas las normas de igual o inferior rango que se opongan a lo establecido en el presente real decreto-ley, y en particular, los siguientes artículos

de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal:

a) El artículo 40.

b) Los artículos 43 al 49, con excepción del artículo 46".

La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Publico, recoge en el Capítulo III de su Título Preliminar *"Disposiciones generales, principios de actuación y funcionamiento del sector público",* los principios de la potestad sancionadora, señalando en su artículo 26, relativo a la *"Irretroactividad"* que:

"1. Serán de aplicación las disposiciones sancionadoras vigentes en el momento de producirse los hechos que constituyan infracción administrativa.

2. Las disposiciones sancionadoras producirán efecto retroactivo en cuanto favorezcan al presunto infractor o al infractor, tanto en lo referido a la tipificación de la infracción como a la sanción y a sus plazos de prescripción, incluso respecto de las sanciones pendientes de cumplimiento al entrar en vigor la nueva disposición".

Por otra parte, la LOPD en su artículo 48.3 dispone que *"los procedimientos sancionadores tramitados por la Agencia Española de Protección de Datos, en ejercicio de las potestades que a la misma atribuyan esta u otras Leyes, salvo los referidos a infracciones de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, tendrán una duración máxima de seis meses."*

El Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, señala en su artículo 126:

"1. Finalizadas las actuaciones previas, éstas se someterán a la decisión del Director de la Agencia Española de Protección de Datos.

Si de las actuaciones no se derivasen hechos susceptibles de motivar la imputación de infracción alguna, el Director de la Agencia Española de Protección de Datos dictará resolución de archivo que se notificará al investigado y al denunciante, en su caso.

2. En caso de apreciarse la existencia de indicios susceptibles de motivar la imputación de una infracción, el Director de la Agencia Española de Protección de Datos dictará acuerdo de inicio de procedimiento sancionador o de infracción de las Administraciones públicas, que se tramitarán conforme a lo dispuesto, respectivamente, en las secciones tercera y cuarta del presente capítulo".

Y el artículo 122, señala que:

"1. Con anterioridad a la iniciación del procedimiento sancionador, se podrán realizar actuaciones previas con objeto de determinar si concurren circunstancias que justifiquen tal iniciación. En especial, estas actuaciones se orientarán a determinar, con la mayor precisión posible, los hechos que pudieran justificar la incoación del procedimiento, identificar la persona u órgano que pudiera resultar responsable y fijar las circunstancias relevantes que pudieran concurrir en el caso.

2. Las actuaciones previas se llevarán a cabo de oficio por la Agencia Española de Protección de Datos, bien por iniciativa propia o como consecuencia de la existencia de una denuncia o una petición razonada de otro órgano.

3. Cuando las actuaciones se lleven a cabo como consecuencia de la existencia de una denuncia o de una petición razonada de otro órgano, la Agencia

Española de Protección de Datos acusará recibo de la denuncia o petición, pudiendo solicitar cuanta documentación se estime oportuna para poder comprobar los hechos susceptibles de motivar la incoación del procedimiento sancionador.

4. Estas actuaciones previas tendrán una duración máxima de doce meses a contar desde la fecha en la que la denuncia o petición razonada a las que se refiere el apartado 2 hubieran tenido entrada en la Agencia Española de Protección de Datos o, en caso de no existir aquéllas, desde que el Director de la Agencia acordase la realización de dichas actuaciones.

El vencimiento del plazo sin que haya sido dictado y notificado acuerdo de inicio de procedimiento sancionador producirá la caducidad de las actuaciones previas".

Consta en el expediente administrativo que el escrito de denuncia de fecha 06/02/2018 tuvo entrada en esta AGPD el 13/02/2018, llevándose a cabo con posterioridad actuaciones previas al objeto de determinar si concurrían circunstancias que justificaran la iniciación del procedimiento sancionador correspondiente.

El procedimiento sancionador nº PS/00243/2018 se inició mediante acuerdo de la Directora de la Agencia Española de Protección de Datos de fecha 07/06/2018, prácticamente cuatro meses después, notificándose a la denunciada COMMCENTER en la misma fecha, por lo que de conformidad con lo señalado en la Disposición Transitoria Primera del R.D. Ley 5/2018, que regula el régimen transitorio de los procedimientos, al haberse iniciado el procedimiento antes de su entrada en vigor por lo que no procede estimar la alegación formulada.

Como se ha señalado con anterioridad, invocaba la representación del recurrente la nulidad de pleno derecho del artículo 45 de la LOPD al haber sido derogado por el anterior R.D. en base al artículo 47.2 de la Ley 39/2015, que señala: *"2. También serán nulas de pleno derecho las disposiciones administrativas que vulneren la Constitución, las leyes y otras disposiciones administrativas de rango superior, las que regulen materias reservadas a la Ley, y las que establezcan la retroactividad de disposiciones sancionadoras no favorables o restrictivas de derechos individuales".*

La entrada en vigor el 25/05/2018 del RGPD supuso la derogación de la LOPD y de su Reglamento de desarrollo, salvo en todas aquellas cuestiones no reguladas por aquél que no se opusieran al mismo.

En la exposición de motivos del Real Decreto-Ley antes citado se señala *"la necesidad de adaptar el marco normativo interno al Reglamento General de Protección de Datos supuso la aprobación por el Consejo de Ministros en su sesión de 10 de noviembre de 2017 de un proyecto de ley orgánica, remitido a las Cortes Generales, que actualmente se encuentra en tramitación parlamentaria".*

No obstante, si bien el reglamento europeo establece un régimen sancionador aplicable en España, no regula cuestiones tan esenciales como los plazos de prescripción, las sanciones, etc., al considerar que deben fijarse en el ordenamiento interno de los Estados, factores que son básicos para garantizar la seguridad jurídica de los procedimientos y proteger de manera efectiva los derechos de los ciudadanos; es decir, existen determinadas cuestiones que no son objeto de reserva de ley orgánica y que resulta imprescindible la adopción urgente de una norma con rango de ley que permita la adaptación del derecho español del reglamento europeo.

Por tanto, se trata de una norma provisional que se dicta a la espera de la Ley Orgánica ahora mismo en tramitación, que realiza dicha adaptación y que tendrá vigencia sólo hasta el momento en el que las Cortes aprueben el proyecto de ley en tramitación.

Es por ello que el Real Decreto-ley entra a regular aspectos relacionados con la inspección, el régimen sancionador, procedimiento de instrucción, etc., y que son relevantes para la garantía efectiva del derecho a la protección de los datos personales, dado que aportan seguridad jurídica.

Es en dicho ámbito donde hay que entender la derogación normativa contenida en el mismo y en particular los artículos de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal: a) El artículo 40 y b) Los artículos 43 al 49, con excepción del artículo 46.

Como continuaba señalando la Exposición de Motivos *"…el real decreto-ley representa un instrumento constitucionalmente licito, en tanto que pertinente y adecuado para la consecución del fin que justifica la legislación de urgencia, que no es otro, tal como reiteradamente ha exigido nuestro Tribunal Constitucional, que subvenir a una situación concreta, dentro de los objetivos gubernamentales, que por razones difíciles de prever requiere una acción normativa inmediata en un plazo más breve que el requerido por la vía normal…"*

Los hechos que constituían el presupuesto fáctico de la imputación dirigida contra la entidad se encuadraban, al tiempo de su comisión por la recurrente, en el tipo sancionador previsto en el artículo 44.4.h) de la LOPD, infracción grave para la que el artículo 45.2 de la LOPD preveía una sanción con multa de 40.001 a 300.000 €.

Se desprende que tras la entrada en vigor del nuevo RGPD -Reglamento (UE) 2016/679 - de 25/05/2016, aunque su plena aplicación se produce a partir del 25/05/2018, ha incidido en la gravedad de la conducta que ahora se enjuicia, influyendo en la sanción a imponer por los mismos hechos pudiendo alcanzar la cuantía de 10.000.000 € como máximo o, tratándose de una empresa, en cuantía equivalente al 2% como máximo de su volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía, de conformidad con lo señalado en el artículo 83.4 del RGPD.

Resulta conveniente en todo caso, al hilo de la cuestión examinada, recordar que la aplicación del principio de retroactividad de la norma sancionadora más favorable obliga a aplicar en bloque y no parcialmente la norma que tenga tal condición. Así lo ha reconocido reiteradamente el Tribunal Constitucional, que en su STC 75/2002 declaraba *" ...ya en la sentencia del Tribunal Constitucional 131/1986, de 29 de octubre, (RTC1986,131), fundamento jurídico 2, tuvimos ocasión de decir que el principio de retroactividad de la Ley penal más favorable (...) supone la aplicación integra de la Ley más beneficiosa, incluidas aquellas de sus normas que puedan resultar perjudiciales en relación con la Ley anterior, que se desplaza en virtud de dicho principio, siempre que el resultado final como es obvio, suponga beneficio para el reo".*

En consecuencia, a tenor del principio de retroactividad de la disposición sancionadora más favorable, y dado que la entrada en vigor del RGPD incide en la gravedad de la infracción imputada al recurrente, pudiendo la sanción alcanzar una cuantía mayor se estima conveniente mantenerla como se dictó en la resolución acordada en el procedimiento sancionador incoado n° PS/00243/2018.

IV

En segundo lugar, la representación del recurrente ha alegado que en todo momento actúa en la condición de encargado del tratamiento por cuenta de TELEFONICA por lo que no se le puede considerar como responsable del tratamiento dado que tal consideración le provoca indefensión.

Dando por sentado lo alegado por dicha representación y que el recurrente es el encargado del tratamiento, hay que señalar que la LOPD, en su artículo 43, atribuye la condición de responsables de las infracciones a los responsables de los ficheros y a los encargados de tratamiento: *"Los responsables de los ficheros y los encargados de los tratamientos estarán sujetos al régimen sancionador establecido en la presente Ley"*. Por tanto, ambas figuras están sujetas al régimen sancionador de la LOPD.

Conforme al artículo 3.d) de la LOPD, el responsable del fichero o del tratamiento es *"la persona física o jurídica... que decida sobre la finalidad, contenido y uso del tratamiento".* En el artículo 5.1.q) del RDLOPD se define *"Responsable del fichero o del tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente".*

El artículo 3.g) de la LOPD, define la figura del encargado del tratamiento como *"… la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento…".*

Y el artículo 5.1.i) del RDLOPD lo define como *"La persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio".*

Es cierto, que en virtud de la adhesión al contrato aportado la entidad recurrente estaba obligada a verificar que entre los datos personales solicitados se encontraba la dirección de correo electrónico, al ser este dato preceptivo y necesario para poder continuar con la operación de financiación, ya que era a esta dirección a la que se enviaba la copia del contrato de financiación y las condiciones generales y, además, que cuando un cliente no tenía dirección de correo electrónico se le creaba una nueva en el terminal que compra.

Ante la respuesta ofrecida a los inspectores de la AEPD, éstos mostraron al representante de la entidad la copia de 13 solicitudes de contrato en las que constaba haber sido tramitadas en el establecimiento del recurrente. El representante de la entidad respondió desconocer el motivo por el que en dichas solicitudes de financiación aparecía la dirección de correo electrónico ****EMAIL.1*.

Por tanto, consta acreditado que el recurrente incumplió su obligación de fiscalizar la veracidad o no de la documentación aportada, desconociendo porque en las solicitudes de financiación figuraba la dirección de correo electrónico del denunciante, dirección que obviamente no correspondía a los clientes-solicitantes e ignorando el motivo por el que las solicitudes de financiación se remitieron a la dirección de correo electrónico ***EMAIL.1 permitiendo el acceso no autorizado por parte de terceros a los datos personales, lo que denota una falta de diligencia grave. En este sentido interpreta el art. 12.4 de la LOPD la sentencia de 17/05/2013 de la A.N., recurso 25/2010, cuando señala *"A mayor abundamiento, además, y como*

igualmente hemos sostenido en la Sentencia de 13 de abril de 2005 (recurso nº. 241/2003) lo que determina la Ley Orgánica 15/1999 en el art. 12.4 que invoca la parte demandante, es que en caso de que el encargado del tratamiento destine los datos a una finalidad distinta a la indicada, los comunique o los utilice incumpliendo las estipulaciones del contrato "...será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente". El término "también" que utiliza el precepto deja claro que no se establece allí un mecanismo de sustitución ni de derivación de responsabilidades sino de agregación, pues el responsable del fichero no pierde su condición de tal ni queda exonerado de responsabilidad por el hecho de que al encargado del tratamiento que incumpla lo estipulado se le atribuya "también" la consideración de responsable del tratamiento" (el subrayado es de la AEPD).

Por lo que el término *"también"* que utiliza el precepto deja claro que no se establece allí un mecanismo de sustitución ni de derivación de responsabilidades sino de agregación, pues el responsable del fichero no pierde su condición de tal, ni queda exonerado de responsabilidad por el hecho de que al encargado del tratamiento, que incumpla lo estipulado, se le atribuya *"también"* la consideración de responsable del tratamiento.

V

Por último, la representación de la recurrente ha manifestado que la resolución recurrida elude por completo las pruebas de cumplimiento por la empresa de las obligaciones exigibles en base a la LOPD y su normativa de desarrollo.

Sin embargo, tal alegato no puede ser admitido ni aceptado, puesto que lo que la citada representación pretende es dar carta de naturaleza y equiparar con una suerte de eximente de responsabilidad al cumplimiento de obligaciones que vienen determinadas en la normativa aplicable y como no podría ser de otra forma.

Pero, además, de las medidas enumeradas por la entidad ninguna de ellas ha sido cumplida a satisfacción en virtud de las citadas obligaciones: no se verificaron correctamente los datos por parte de la entidad, como ya ha sido puesto de relieve.

También ha sido puesto de manifiesto que el presente procedimiento trae causa de la elusión de medidas específicamente destinadas a impedir el acceso no autorizado por parte de terceros a los datos personales de sus ficheros, por lo que argüir el cumplimiento de las obligaciones establecidas en la normativa sobre protección de datos y la correcta implantación de medidas de seguridad se revela un sinsentido.

Y, para finalizar, en cuanto al papel del encargado del tratamiento, su incorrecta consideración y la actuación bajo las estrictas directrices del responsable ya ha sido argumentado y rebatido con anterioridad.

IV

En consecuencia, en el presente recurso de reposición, el recurrente no ha aportado nuevos hechos o argumentos jurídicos que permitan reconsiderar la validez de la resolución impugnada.

Vistos los preceptos citados y demás de general aplicación,

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

PRIMERO: DESESTIMAR el recurso de reposición interpuesto por **COMMCENTER, S.A.** contra la Resolución de esta Agencia Española de Protección de Datos dictada con fecha 03/10/2018, en el procedimiento sancionador PS/00243/2018.

SEGUNDO: NOTIFICAR la presente resolución a la entidad **COMMCENTER, S.A.**

TERCERO: Advertir al sancionado que la sanción impuesta deberá hacerla efectiva una vez sea ejecutiva la presente resolución, de conformidad con lo dispuesto en el artículo 98.1.b) de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, en el plazo de pago voluntario que señala el artículo 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 en la cuenta restringida nº ES00 0000 0000 0000 0000 0000, abierta a nombre de la Agencia Española de Protección de Datos en el Banco CAIXABANK, S.A. o 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 apartado 2 del artículo 37 de la LOPD, en la redacción dada por el artículo 82 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, la presente Resolución se hará pública, una vez haya sido notificada a los interesados. La publicación se realizará conforme a lo previsto en la Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones y con arreglo a lo dispuesto en el artículo 116 del reglamento de desarrollo de la LOPD aprobado por el Real Decreto 1720/2007, de 21 diciembre.

Contra esta resolución, que pone fin a la vía administrativa, se podrá interponer 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 Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, 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 del referido texto legal.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) 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 LPACAP. 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