- **Expediente N.º: EXP202408867**

RESOLUCIÓN DE TERMINACIÓN DEL PROCEDIMIENTO POR RECONOCIMIENTO DE RESPONSABILIDAD Y PAGO VOLUNTARIO

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

ANTECEDENTES

PRIMERO: Con fecha 10 de enero de 2026, la Presidencia de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a ***DÉCIMAS, S.L.*** (en adelante, ***DÉCIMAS***), mediante el acuerdo que se transcribe:

<<
Expediente N.º: EXP202408867

ACUERDO DE INICIO DE PROCEDIMIENTO SANCIONADOR

De las actuaciones practicadas por la Agencia Española de Protección de Datos y en base a los siguientes

HECHOS

PRIMERO: Con fecha 10 y 14 de mayo de 2024 se han interpuesto dos reclamaciones ante la Agencia Española de Protección de Datos por una posible infracción imputable a **DÉCIMAS, S.L.** con NIF **B78785219** (en adelante, DÉCIMAS).

Los hechos que se pone en conocimiento de esta autoridad son:

Los reclamantes manifiestan que han recibido un correo electrónico en el que la parte reclamada le informa de que ha sufrido una incidencia de seguridad que ha afectado a su base de datos y que, como consecuencia de esta, sus datos personales (nombre y apellidos, dirección de correo electrónico y DNI) se han visto expuestos.

Junto a los escritos de reclamación, se aporta:

-Copia del correo electrónico remitido el 10 de mayo de 2024 por la parte reclamada informando de la brecha sufrida.

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 de dicha reclamación a DECIMAS 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 notificación del traslado de la reclamación, que se practicó conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), fue realizada en fecha 18/06/2024 como consta en el acuse de recibo que obra en el expediente.

Con fecha 17/07/2024 se recibe en esta Agencia escrito de respuesta en el que se indica lo siguiente:

*"(...) La entidad ***EMPRESA.1 es encargada del tratamiento de la entidad DÉCIMAS, S.L.U. siendo la primera quien sufre la incidencia de seguridad. Sin embargo, efectivamente, la entidad DÉCIMAS, S.L.U es la responsable del tratamiento de los datos personales del reclamante (…)*

A continuación, se describen detallada y cronológicamente los hechos:

*1 El 26 de abril de 2024 a las 9:42 horas DÉCIMAS, S.L.U. recibe un mensaje de INCIBE comunicándonos un posible ataque a nuestra base de datos con la aparición de un mensaje publicado el 25 de abril de 2024 a las 18:12 por el usuario ***USUARIO.1 ofreciendo a la venta los supuestos datos.*
*2 El 26 de abril de 2024 a las 10:59 horas desde DÉCIMAS, S.L.U. reenviamos el mensaje a ***EMPRESA.1*
*3 El 26 de abril de 2024 a las 13:00 horas ***EMPRESA.1 contrata un informe forense de vulnerabilidad.*
*4 El 26 de abril de 2024 a las 15:00 horas ***EMPRESA.1 nos confirma que se trata de una violación y nos recomienda la comunicación a la Agencia Española de Protección de Datos.*
5 El 26 de abril de 2024 a las 17:55 horas desde DÉCIMAS, S.L.U presentamos comunicación inicial a la Agencia a través de la sede electrónica.
6 El 26 de abril de 2024 a las 20:58 horas queda solucionado el ataque.
*7 El 27 de abril de 2024 ***EMPRESA.1 se comunica con INCIBE para confirmar que las medidas aplicadas son las correctas recibiendo confirmación y la solicitud de las IPs si fuera posible.*
*8 El día 28 de abril a las 22:02 horas ***EMPRESA.1 traslada a INCIBE la lista de las IPs encontradas.*
*(…) se adjunta al presente escrito copia del Informe desarrollado por NACATA SECURITY, una empresa tercera independiente, a quien ***EMPRESA.1 contrata para realizar una auditoría de seguridad y dar solución a la incidencia ese mismo día.*

*Dicho informe recoge que, ante los indicios de un posible ciberataque, ***EMPRESA.1 les solicita una revisión de seguridad sobre un endpoint en uno de los entornos web: (...). Se registra que este endpoint había recibido varias peticiones con inyección de payloads maliciosos, cuyo aparente objetivo es ejecutar código en el sistema de forma remota.*

A pesar de las medidas de seguridad implementadas se detecta, a través de los logs, una fuga de información de las bases de datos mediante técnicas de inyección de código SQL. La Inyección SQL es un método de infiltración de código intruso que se

vale de una vulnerabilidad informática presente en una aplicación en el nivel de validación de las entradas para realizar operaciones sobre una base de datos.

El origen de la vulnerabilidad radica en la incorrecta comprobación o filtrado de las variables utilizadas en un programa que contiene, o bien genera, código SQL. Es, de hecho, un error de una clase más general de vulnerabilidades que puede ocurrir en cualquier lenguaje de programación o script que esté incrustado en otro. Se conoce como Inyección SQL, indistintamente, al tipo de vulnerabilidad, al método de infiltración, al hecho de incrustar código SQL intruso y a la porción de código incrustado".(…)
Número de personas afectadas por la violación de seguridad de los datos personales:
*1 Correo electrónico: ***CANTIDAD.1 emails, de los cuales más de ***CANTIDAD.2 son SPAM.*
*2 Fecha de nacimiento: ***CANTIDAD.3 personas.*
*3 Género: ***CANTIDAD.4 personas.*
*4 DNI: ***CANTIDAD.5 personas. (…)*
Datos afectados por la violación de seguridad de los datos personales:
1 ***(…),*** *que corresponde al correo electrónico de el/la interesado/a*
2 ***(…),*** *que corresponde al género de el/la interesado/a*
3 ***(…),*** *que corresponde al apellido de el/la interesado/a*
4 ***(…),*** *que corresponde al nombre de el/la interesado/a*
5 ***(…),*** *que corresponde al segundo nombre de el/la interesado/a*
6 Fecha de nacimiento
7 DNI

8 *Cabe señalar que las contraseñas son firmas encriptadas, en ningún caso la contraseña en claro. Tampoco se filtraron direcciones (default_shipping y default_billing son ids, pero no información filtrada)(…)*

a pesar de las medidas de seguridad implementadas, se detectó a través de los logs una fuga de información de las bases de datos mediante técnicas de inyección de código SQL. Por ello, durante la revisión de seguridad se recreó la explotación de la vulnerabilidad para identificarla, y se parcheó satisfactoriamente con fecha 26 de abril de 2024.
En el citado documento se recogen las siguientes medidas para evitar ataques de inyección de SQL en el futuro tales como:

(…)

TERCERO: Con fecha 27 de julio de 2024, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación.

CUARTO: 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 las funciones asignadas a las autoridades de control en el artículo 57.1 y de los poderes otorgados en el artículo 58.1 del Reglamento (UE)

2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VIII, de la LOPDGDD.

Como consecuencia de las actuaciones realizadas, se ha tenido conocimiento de los siguientes extremos:

1.- Análisis de la brecha.

1.1. Notificaciones presentadas ante la AEPD.

Complementariamente a las reclamaciones recibidas, la brecha fue notificada por DÉCIMAS en calidad de responsable del tratamiento.

Resumen de las notificaciones presentadas:

- Notificación inicial recibida el 26 de abril de 2024, notificación completa recibida el 14 de mayo de 2024.
- ***(…).***
- Tipología de los datos según notificación: datos básicos (nombre, apellidos, fecha de nacimiento), DNI, NIE, pasaporte y / o cualquier otro documento identificativo, datos de contacto.
- ***(…)***
- Fecha de inicio de la brecha el 24 de abril de 2024.
- Fecha de detección de la brecha el 26 de abril de 2024.
- Se ha comunicado la brecha a los afectados en fecha 3 de mayo de 2024.
- Encargado del tratamiento: ******EMPRESA.1.***

1.2. Descripción y cronología de los hechos.

(…)

1.3. Impacto de la brecha. Posibles consecuencias para los afectados.

- ***(…)***

La valoración que emite la parte reclamada sobre el incidente es la siguiente: "*DÉCIMAS, S.L.U. considera que las personas no se verán afectadas o pueden encontrar algunos inconvenientes muy limitados y reversibles que superarán sin ningún problema.*
Como ejemplo de ello, molestias o irritaciones en caso de que sus datos se hubieran exfiltrado, y pudieran ser utilizados para el envío de comunicaciones comerciales.

Asimismo, cabe mencionar que, desde el pasado mes de mayo cuando se comunicó la incidencia a los interesados hasta la fecha de envío de la contestación a la Agencia al "Traslado de reclamación y solicitud de información", a DÉCIMAS, S.L.U. no le consta que se haya materializado inconveniente o perjuicio alguno sobre los interesados afectados por la incidencia de seguridad."

2.- Comunicación a los afectados.

DÉCIMAS ha comunicado la brecha a los afectados mediante correo electrónico, entre los días 3 y 10 de mayo de 2024. La brecha fue comunicada a 331.809 usuarios de los que se disponía de su correo electrónico. Se aporta acreditación del envío masivo de correos, donde aproximadamente el 96% fueron remitidos correctamente.

Se aporta copia de la comunicación remitida, en la que se informa del incidente ocasionado ("*hemos detectado una incidencia de seguridad que afectó a nuestra base de datos de clientes web*"), la tipología de datos afectados ("*nombre y apellidos, dirección de correo electrónico y DNI, en ningún caso a números de teléfono ni datos bancarios de ningún tipo*") y las medidas adoptadas a alto nivel. Se facilita a los afectados un correo electrónico de contacto y unas recomendaciones de seguridad para prevenir posibles intentos de fraude.

Complementariamente, en una de las reclamaciones recibidas consta una comunicación idéntica, por lo que se puede acreditar la efectividad de la comunicación en base a esa muestra.

3.- Medidas de seguridad.

3.1. Medidas implantadas con anterioridad a la brecha.

(…)

3.2. Motivo por el cual las medidas de seguridad implantadas no han impedido el incidente.

(…)

3.3. Medidas técnicas y organizativas adoptadas para evitar incidentes como el sucedido.

- ***(…)***

4.- Tratamiento de datos.

4.1. Roles desempeñados.

DÉCIMAS manifiesta la siguiente información aclaratoria sobre los roles desempeñados con relación a esta brecha: "*La entidad* ******EMPRESA.1*** *es encargada del tratamiento de la entidad DÉCIMAS, S.L.U. siendo la primera quien sufre la*

incidencia de seguridad. Sin embargo, efectivamente, la entidad DÉCIMAS, S.L.U es la responsable del tratamiento de los datos personales del reclamante."

Por otra parte, se indica la siguiente información relativa a la entidad ******EMPRESA.2, ,*** (en adelante, ******EMPRESA.2***) puesto que como se indicará posteriormente, figura en cierta documentación facilitada: "*DÉCIMAS, S.L.U. es una sociedad perteneciente al grupo empresarial cuya sociedad matriz es* ******EMPRESA.2*** *En el contexto de la brecha de seguridad notificada, la entidad responsable del tratamiento de los datos personales afectados es DÉCIMAS, S.L.U., por ser quien determina los fines y medios del tratamiento.* ******EMPRESA.2****, como sociedad matriz, presta determinados servicios generales de apoyo a DÉCIMAS, S.L.U., incluyendo soporte jurídico, informático (IT) y otros servicios corporativos centralizados, en virtud de un contrato de prestación de servicios intragrupo firmado entre ambas entidades. No obstante,* ******EMPRESA.2*** *no adopta decisiones autónomas sobre los tratamientos de datos personales realizados por DÉCIMAS, ni actúa como responsable conjunto, sino que desarrolla funciones de soporte dentro del marco de funcionamiento común del grupo empresarial.*"

4.2. Contrato de encargo de tratamiento.

Se aporta contrato de encargo de tratamiento suscrito entre ******EMPRESA.1*** y ******EMPRESA.2*** a fecha 3 de febrero de 2020. En este contrato, se comprueba que constan, entre otros aspectos:

- El objeto del contrato es la prestación de servicio de desarrollos informáticos y su mantenimiento. Los servicios se denominan "*alojamiento y mantenimiento AWS*" y "*mantenimiento WEB mensual*", cuyos fines son potenciar la venta online y agilizar procesos de negocio.

- El tratamiento de datos de las sociedades vinculadas a ******EMPRESA.2,*** entre las que se cita a DÉCIMAS, son inherentes para la prestación de estos servicios.

- Entre las obligaciones del encargado consta el "*tratar los datos de acuerdo con las instrucciones dadas por el responsable del tratamiento*".

- ***(…).***

Adicionalmente, DÉCIMAS aporta contrato suscrito entre su entidad y ******EMPRESA.2***, fechado a 1 de enero de 2016. Se observan los siguientes aspectos relevantes de la documentación facilitada:

- Se trata de un contrato de servicios intra-grupo, donde además de DÉCIMAS, figuran otras terceras entidades ***(***EMPRESA.3 y ***EMPRESA.4). ***EMPRESA.2*** tiene la consideración de proveedor y el resto de las entidades de clientes.

- Proveedor y clientes forman parte del grupo denominado ******EMPRESA.2***. Se indica que: "*por razones de estrategia empresarial y con el fin de racionalizar sus recursos, los Clientes están interesados en recibir del proveedor*

determinados servicios considerados necesarios, útiles y beneficiosos para la actividad de los clientes", encomendándole su gestión.

- La duración del contrato se estipula en 3 años, pudiendo ser renovado anualmente de forma tácita.

- Relativo a la protección de datos, se indica que el proveedor tratará la información de conformidad con las instrucciones que el cliente proporcione.

- ***(…).***

4.3. Otros aspectos.

Se aportan copias de los registros de actividades de tratamiento tanto de DÉCIMAS como de ******EMPRESA.1***:

- Para el caso de DÉCIMAS, el registro fue actualizado el 11 de julio de 2024 según manifestaciones. Entre las actividades consta una referida a clientes, donde figuran las categorías de datos objeto de tratamiento, entre las que se incluyen las afectadas (así como algunas adicionales, referidas datos financieros y medios de pago).

- Por parte de ***EMPRESA.1, el registro de actividades de tratamiento se encuentra fechado a 18 de octubre de 2021. Entre los fines consta, entre otros "*Gestión y prestación del servicio contratado por parte de los clientes.".* No se localiza ninguna referencia específica a DÉCIMAS en el registro, siendo una descripción de carácter más general.

5.- Publicación de los datos exfiltrados en Internet.

(…)

QUINTO: De acuerdo con el informe recogido de la herramienta AXESOR, la entidad DÉCIMAS es una empresa constituida en el año 1988, y con un volumen de negocios de 182.684.031euros en el año 2024.

FUNDAMENTOS DE DERECHO

I

Competencia

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

iniciar y resolver este procedimiento la Presidencia de la Agencia Española de Protección de Datos.

II

Procedimiento

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

De acuerdo con el artículo 64 de la LOPDGDD, y teniendo en cuenta las características de la presunta infracción cometida, se inicia un procedimiento sancionador.

El procedimiento tendrá una duración máxima de doce meses a contar desde la fecha del acuerdo de inicio. Transcurrido ese plazo se producirá su caducidad y, en consecuencia, el archivo de actuaciones, de conformidad con lo establecido en el artículo 64 de la LOPDGDD.

Si en el plazo estipulado no efectuara alegaciones a este acuerdo de inicio, el mismo podrá ser considerado propuesta de resolución, según lo establecido en el artículo 64.2.f) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo, LPACAP).

III

Cuestiones previas

El artículo 4.1) del RGPD, define «dato personal» como: "toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona".

El artículo 4.2) del RGPD, define «tratamiento» como: "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción."

El artículo 4.7) del RGPD, define al «responsable del tratamiento» o «responsable» como: "la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros". A su vez el artículo 4.8) del RGPD determina al «encargado del tratamiento» o «encargado» como la

persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

En el presente caso, de acuerdo con lo establecido en el artículo 4.1 y 4.2 del RGPD, consta la realización de un tratamiento de datos personales, toda vez que DÉCIMAS realiza, entre otros tratamientos, la recogida y conservación de datos personales de personas físicas: nombre y apellidos, fecha de nacimiento, correo electrónico, género y DNI.

Por otro lado***, ***EMPRESA.1*** realiza esta actividad en su condición de encargado del tratamiento, dado que trata los datos personales por cuenta del responsable del tratamiento, en virtud del artículo 4.8 del RGPD.

IV
Obligación incumplida. Integridad y confidencialidad

La letra f) del artículo 5.1 del RGPD propugna:

"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»)."

Según las Directrices sobre la notificación de las violaciones de la seguridad de los datos personales de acuerdo con el Reglamento 2016/679 del GT29 se produce una «violación de la confidencialidad» cuando se produce una revelación no autorizada o accidental de los datos personales, o el acceso a los mismos; una «violación de la integridad»: cuando se produce una alteración no autorizada o accidental de los datos personales; y una «violación de la disponibilidad»: cuando se produce una pérdida de acceso accidental o no autorizada a los datos personales, o la destrucción de los mismos.

El principio de confidencialidad recogido en citado artículo 5.1 f) del RGPD, obliga a los responsables del tratamiento a garantizar que los datos personales sean tratados de forma que se garantice la confidencialidad de los datos personales, evitando accesos no autorizados, usos indebidos o divulgación a terceros no autorizados. Ello exige implementar medidas técnicas y organizativas apropiadas de todo tipo para proteger los datos frente a posibles brechas de datos personales, tanto externas como internas. Dichas medidas deben ser adecuadas para evitar que se materialicen los riesgos en los derechos y libertades de las personas físicas que puedan derivarse del tratamiento, y deben ser revisadas y actualizadas periódicamente para garantizar su eficacia.

En el presente caso, consta la existencia de una brecha de datos personales que se ha materializado en una pérdida de confidencialidad, ocasionada por un ciberataque ocurrido en abril de 2024 a ciertas URLs públicas del entorno web de DÉCIMAS (https://www.decimas.com), desarrollado y operado por el encargado del tratamiento,

EMPRESA.1, notificada inicialmente a esta Agencia el 26 de abril de 2024 y posteriormente complementada el 14 de mayo de 2024. La tipología del ataque fue de inyección de SQL que permitió al atacante realizar una exfiltración masiva de los datos de clientes alojados en el sistema afectado. En el momento de los hechos, DECIMAS no contaba con ***(…).

El 26 de abril de 2024 a las 9:42 horas DÉCIMAS, S.L.U. recibe un mensaje de INCIBE comunicando un posible ataque a la base de datos de DÉCIMAS con la aparición de un mensaje publicado el 25 de abril de 2024 a las 18:12 por el usuario ******USUARIO.1*** ofreciendo a la venta los datos exfiltrados. Por lo tanto, el conocimiento de que el ataque se estaba produciendo fue mediante información proporcionada por una entidad externa, en este caso el INCIBE, y no por una detección realizada por la entidad afectada, DECIMAS. Circunstancia que aventura la falta de medidas de seguimiento relacionadas con la detección de ataques al objeto de su rápida solución.

El impacto de la brecha se estima en el compromiso de los siguientes datos personales:

- Correo electrónico: ******CANTIDAD.1*** emails, de los cuales más de ******CANTIDAD.2*** son SPAM
- Fecha de nacimiento: ******CANTIDAD.3*** personas
- Género: ******CANTIDAD.4*** personas
- DNI: ******CANTIDAD.5*** personas

En el caso que nos ocupa, de las actuaciones de investigación realizadas por la presente autoridad, se desprende una presunta vulneración del principio de confidencialidad manifestada con el acceso por parte de terceros no autorizados a datos personales que estaban siendo objeto de tratamiento y a la publicación de los mismos en internet.

Así pues, se destaca la insuficiencia de las siguientes medidas técnicas y organizativas que facilitaron la materialización y extensión en el tiempo de la brecha de datos personales:

En primer lugar, se subraya la ausencia de medidas destinadas a la alerta temprana de incidentes, así como de monitorización de vulnerabilidades. Como se ha señalado, el Informe de revisión de seguridad web realizada por la entidad independiente NACATA SECURITY, S.L remitido por DÉCIMAS a esta Agencia con fecha 26 de abril de 2024:"… *El origen de la vulnerabilidad radica en la incorrecta comprobación o filtrado de las variables utilizadas en un programa que contiene, o bien genera, código SQL. Es, de hecho, un error de una clase más general de vulnerabilidades que puede ocurrir en cualquier lenguaje de programación o script que esté incrustado en otro. Se conoce como Inyección SQL, indistintamente, al tipo de vulnerabilidad, al método de infiltración, al hecho de incrustar código SQL intruso y a la porción de código incrustado".*

Dicha vulnerabilidad tiene un impacto trascendente en la seguridad de la aplicación, lo que podría llegar a comprometerla de forma severa.

Durante la revisión de seguridad se recreó la explotación de la vulnerabilidad para identificarla, y se parcheó satisfactoriamente con fecha 26 de abril de 2024. La prueba de que se trataba de una vulnerabilidad de carácter más general es que, el mismo día en que se le notificó la incidencia por el INCIBE, esta fue solucionada.

A lo anterior, debe añadirse que tal y como se señala en el informe de revisión de seguridad web "***…(…)***."

Todo ello pone de manifiesto que DÉCIMAS no tenía implantada medidas adecuadas destinada a comprobar la existencia de vulnerabilidades ni de alerta temprana de incidentes, por lo que carecía de una monitorización adecuada de sus sistemas. Esta ausencia de controles permitió que un atacante accediera y exfiltrara los datos personales de los clientes. Una ausencia de controles que, como ya hemos indicado, también se evidencia por el hecho de que INCIBE comunicara a DECIMAS la incidencia.

Por otro lado, como se indica, los hechos se han materializado en una pérdida de confidencialidad provocada, entre otras, por la ausencia de medidas destinadas a proteger la confidencialidad de los datos objeto de tratamiento, como podría ser medidas de cifrados, de las que se carecía. Así, de acuerdo con los resultados de las actuaciones previas de investigación, ***(…).".***

Finalmente, y aunque se adoptaron medidas con posterioridad a la brecha, resulta llamativo que, meses después del incidente, a principios del año 2025, se realizaron pruebas de intrusión internas y externas, cuyos resultados se reflejan de la siguiente manera: ***(…).*** De lo anterior puede concluirse que el dominio de DECIMAS empleado para la materialización de la brecha, tiempo después de que la misma se produjese y a pesar de las medidas que se decían puestas en marca, siguió adoleciendo de diversas vulnerabilidades, dos de ellas calificadas como de criticidad alta.

Por tanto, de conformidad con las evidencias de las que se dispone en este momento de acuerdo de inicio de procedimiento sancionador, se considera que los hechos conocidos podrían ser constitutivos de una infracción, imputable a **DÉCIMAS**, por vulneración del artículo transcrito anteriormente.

V

Tipificación de la infracción del artículo 5.1.f) del RGPD y calificación a efectos de prescripción

El artículo 83.5 del RGPD tipifica como infracción administrativa la vulneración de los artículos siguientes, que se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20.000.000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

"a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9;
b) los derechos de los interesados a tenor de los artículos 12 a 22;

c) las transferencias de datos personales a un destinatario en un tercer país o una organización internacional a tenor de los artículos 44 a 49;
d) toda obligación en virtud del Derecho de los Estados miembros que se adopte con arreglo al capítulo IX;
e) el incumplimiento de una resolución o de una limitación temporal o definitiva del tratamiento o la suspensión de los flujos de datos por parte de la autoridad de control con arreglo al artículo 58, apartado 2, o el no facilitar acceso en incumplimiento del artículo 58, apartado 1."

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".

A los solos efectos del plazo de prescripción, el artículo 72.1 de la LOPDGDD establece lo siguiente:

"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."

VI

Propuesta de sanción

A fin de determinar la multa administrativa a imponer se han de observar las previsiones de los artículos 83.1 y 83.2 del RGPD, preceptos que señalan:

"1. Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 9 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias.

2. Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:
a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;
b) la intencionalidad o negligencia en la infracción;
c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;
d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;
e) toda infracción anterior cometida por el responsable o el encargado del tratamiento;

f) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;
g) las categorías de los datos de carácter personal afectados por la infracción;
h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida;
i) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;
j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42, y
k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción".

Por su parte, el artículo 76 *"Sanciones y medidas correctivas"* de la LOPDGDD dispone:

"1. Las sanciones previstas en los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679 se aplicarán teniendo en cuenta los criterios de graduación establecidos en el apartado 2 del citado artículo.

2. De acuerdo a lo previsto en el artículo 83.2.k) del Reglamento (UE) 2016/679 también podrán tenerse en cuenta:
a) El carácter continuado de la infracción.
b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.
c) Los beneficios obtenidos como consecuencia de la comisión de la infracción.
d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.
e) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.
f) La afectación a los derechos de los menores.
g) Disponer, cuando no fuere obligatorio, de un delegado de protección de datos.
h) El sometimiento por parte del responsable o encargado, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier interesado".

En el presente caso, considerando la gravedad de la posible infracción, atendiendo especialmente a las consecuencias que su comisión provoca en los afectados, correspondería la imposición de multa, además de la adopción de medidas, si procede.

La multa que se imponga deberá ser, en cada caso individual, efectiva, proporcionada y disuasoria, conforme a lo establecido en el artículo 83.1 del RGPD. Para garantizar estos principios, se considera, con carácter previo, el volumen de negocio de DÉCIMAS de 82.684.031euros en el año 2024.

A efectos de decidir sobre la imposición de una multa administrativa y su cuantía, de conformidad con las evidencias de que se dispone en el presente momento de

acuerdo de inicio de procedimiento sancionador, y sin perjuicio de lo que resulte de la instrucción, se considera que procede graduar la sanción a imponer de acuerdo con las circunstancias siguientes, contempladas en los preceptos antes citados.

Con carácter previo, se estima que concurren las circunstancias siguientes:

- La naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate, así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido (artículo 83.2, letra a), del RGPD): por una exfiltración de datos que afectó a 331.000 interesados según notificación desde el día el 24 de abril de 2024 hasta el 26 de abril de 2024. Es destacable asimismo que el ataque no fuera conocido a través de medios de detección puestos en marcha por DECIMAS, sino gracias a la alerta realizada por una entidad externa, INCIBE que, a su vez, tuvo conocimiento de los hechos por el anuncio publicado en la web referido a la venta de los datos personales obtenidos a resultas del ataque.

- Las categorías de los datos de carácter personal afectados por la infracción (artículo 83.2, letra g), del RGPD): en el presente caso se han obtenido de forma ilícita los datos de correo electrónico, fecha de nacimiento, DNI y género

Por su parte, el tratamiento del número del DNI/NIF/NIE constituye un tratamiento sobre un dato personal de especial sensibilidad, pues permite la identificación directa e inequívoca de una persona física. Tal y como establece el Real Decreto 255/2025, de 1 de abril por el que se regula el Documento Nacional de Identidad, el DNI es un identificador numérico personal de carácter general, con valor suficiente para acreditar tanto la identidad como la nacionalidad del titular, lo que lo convierte en un elemento de especial sensibilidad dentro del ecosistema de datos personales. Además, su utilización indebida conlleva un elevado riesgo de suplantación de identidad, daños patrimoniales o afectación al derecho al honor, riesgos expresamente contemplados en el considerando 75 del RGPD. Por ello, una interpretación sistemática y finalista del RGPD —conforme a los considerandos 51 y 75— permite considerar el número del DNI como un dato particularmente sensible, atendiendo a su capacidad de provocar perjuicios significativos en caso de uso no autorizado. En este sentido, a la hora de valorar esta circunstancia, no solo debe hacerse referencia a los tipos de datos cubiertos por los artículos 9 y 10 del RGPD, sino también a los datos fuera del ámbito de aplicación de estos artículos cuya difusión causa daños o dificultades inmediatas al interesado, tal y como permite el precepto.

Asimismo, se consideran los siguientes factores de graduación en calidad de agravantes:

- La vinculación de la actividad del infractor con la realización de tratamientos de datos personales (artículo 76.2, letra b), de la LOPDGDD): DÉCIMAS es un comercio al por menor de artículos deportivos con miles de

clientes por lo que su actividad requiere un tratamiento continuo de datos personales.

El balance de las circunstancias contempladas en el artículo 83.2 del RGPD y 76.2 de la LOPDGDD, con respecto a la infracción cometida al vulnerar lo establecido en el artículo 5.1.f) del RGPD, permite fijar inicialmente una sanción de multa administrativa de 200.000euros.

VII

Medidas correctivas

De confirmarse la infracción, el citado artículo 77 de la LOPDGDD contempla que la resolución que se dicte pueda establecer las medidas que la entidad infractora deberá adoptar para que cese la conducta infractora, se corrijan los efectos de la infracción que se hubiese cometido y se lleve a cabo la necesaria adecuación, en este caso, a las exigencias contempladas en el artículo 5.1.f del RGPD, debiendo, además, aportar a la AEPD los medios acreditativos del cumplimiento de lo requerido.

Así, se podrá requerir a la entidad responsable para que adecúe su actuación a la normativa de protección de datos personales, con el alcance expresado en los anteriores Fundamentos de Derecho.

En el presente acto se establece cuál es la presunta infracción cometida y los hechos que podrían dar lugar a esa posible vulneración de la normativa de protección de datos, de lo que se infiere con claridad cuáles son las medidas a adoptar, sin perjuicio de que el tipo de procedimientos, mecanismos o instrumentos concretos para implementarlas corresponda a la parte sancionada, pues es el responsable del tratamiento quien conoce plenamente su organización y ha de decidir, en base a la responsabilidad proactiva y en enfoque de riesgos, cómo cumplir con el RGPD y la LOPDGDD.

No obstante, en este caso, con independencia de lo anterior, de conformidad con las evidencias de que se dispone en el presente momento de acuerdo de inicio de procedimiento sancionador, en la resolución que se adopte se podrá requerir a DÉCIMAS para que, en el plazo máximo de 6 meses, a contar desde la fecha de ejecutividad de la resolución finalizadora de este procedimiento, adopte las medidas siguientes:

- Acreditar la aplicación efectiva de las medidas técnicas y organizativas adecuadas para garantizar el cumplimiento del principio confidencialidad en el tratamiento de los datos personales que realiza.

La imposición de esta medida es compatible con la sanción consistente en multa administrativa, según lo dispuesto en el art. 83.2 del RGPD.

Se advierte que no atender la posible orden de adopción de medidas impuestas por este organismo en la resolución del presente procedimiento sancionador podrá ser considerado como una infracción administrativa conforme a lo dispuesto en el RGPD, tipificada como infracción en su artículo 83.5 y 83.6, pudiendo motivar tal conducta la apertura de un ulterior procedimiento administrativo sancionador.

Asimismo, se recuerda que ni el reconocimiento de la infracción cometida ni, en su caso, el pago voluntario de las cuantías propuestas, eximen de la obligación de adoptar las medidas pertinentes para que cese la conducta o se corrijan los efectos de la infracción cometida y la de acreditar ante esta AEPD el cumplimiento de esa obligación

Por lo tanto, a tenor de lo anteriormente expuesto, por la Presidencia de la Agencia Española de Protección de Datos,

SE ACUERDA:

PRIMERO: INICIAR PROCEDIMIENTO SANCIONADOR a **DÉCIMAS, S.L.,** con NIF **B78785219** por la presunta infracción del Artículo 5.1.f) del RGPD, tipificada en el artículo 83.5 del RGPD

SEGUNDO: NOMBRAR como instructora a ***R.R.R.*** y, como secretaria, a ***S.S.S.***, indicando que podrán ser recusadas, en su caso, conforme a lo establecido en los artículos 23 y 24 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP).

TERCERO: INCORPORAR al expediente, a efectos probatorios, la reclamación interpuesta por la parte reclamante y su documentación, así como, así como los documentos obtenidos y generados por la Subdirección General de Inspección de Datos en las actuaciones previas al inicio del presente procedimiento sancionador.

CUARTO: QUE a los efectos previstos en el art. 64.2 b) de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, la sanción que pudiera corresponder sería de multa administrativa de 200.000,00 euros, sin perjuicio de lo que resulte de la instrucción.

QUINTO: NOTIFICAR el presente acuerdo a **DÉCIMAS, S.L**, con NIF **B78785219** otorgándole un plazo de audiencia de diez días hábiles para que formule las alegaciones y presente las pruebas que considere convenientes. En su escrito de alegaciones deberá facilitar su NIF y el número de procedimiento que figura en el encabezamiento de este documento.

De conformidad con lo dispuesto en el artículo 85 de la LPACAP, podrá reconocer su responsabilidad dentro del plazo otorgado para la formulación de alegaciones al presente acuerdo de inicio; lo que llevará aparejada una reducción de un 20% de la sanción que proceda imponer en el presente procedimiento. Con la aplicación de esta reducción, la sanción quedaría establecida en **160.000,00** euros, resolviéndose el procedimiento con la imposición de esta sanción.

Del mismo modo podrá, en cualquier momento anterior a la resolución del presente procedimiento, llevar a cabo el pago voluntario de la sanción propuesta, lo que supondrá la reducción de un 20% de su importe. Con la aplicación de esta reducción, la sanción quedaría establecida en **160.000,00** euros y su pago implicará la

terminación del procedimiento, sin perjuicio de la imposición de las medidas correspondientes.

La reducción por el pago voluntario de la sanción es acumulable a la que corresponde aplicar por el reconocimiento de la responsabilidad, siempre que este reconocimiento de la responsabilidad se ponga de manifiesto dentro del plazo concedido para formular alegaciones a la apertura del procedimiento. El pago voluntario de la cantidad referida en el párrafo anterior podrá hacerse en cualquier momento anterior a la resolución. En este caso, si procediera aplicar ambas reducciones, el importe de la sanción quedaría establecido en **120.000,00 euros**.

En todo caso, la efectividad de cualquiera de las dos reducciones mencionadas estará condicionada al desistimiento o renuncia de cualquier acción o recurso en vía administrativa contra la sanción.

En caso de que optara por proceder al pago voluntario de cualquiera de las cantidades señaladas anteriormente **(160.000,00** euros o **120.000,00 euros**), deberá hacerlo efectivo mediante su ingreso en la cuenta nº ***IBAN: ES00-0000-0000-0000-0000-0000 (BIC/Código SWIFT: CAIXESBBXXX)*** abierta a nombre de la Agencia Española de Protección de Datos en la entidad bancaria CAIXABANK, S.A., indicando en el concepto el número de referencia del procedimiento que figura en el encabezamiento de este documento y la causa de reducción del importe a la que se acoge.

Asimismo, deberá enviar el justificante del ingreso a la Subdirección General de Inspección para continuar con el procedimiento en concordancia con la cantidad ingresada.

En cumplimiento de los artículos 14, 41 y 43 de la LPACAP, se advierte de que, en lo sucesivo, las notificaciones que se le remitan se realizarán exclusivamente de forma electrónica, a través de la Dirección Electrónica Habilitada única (dehu.redsara.es) y de la Sede electrónica (sedeaepd.gob.es), y que, de no acceder a ellas, se hará constar su rechazo en el expediente, dando por efectuado el trámite y siguiéndose el procedimiento. Se le informa que puede identificar ante esta Agencia una dirección de correo electrónico para recibir el aviso de puesta a disposición de las notificaciones y que la falta de práctica de este aviso no impedirá que la notificación sea considerada plenamente válida.

Por último, se señala que conforme a lo establecido en el artículo 112.1 de la LPACAP, contra el presente acto no cabe recurso administrativo alguno.

1479-021025

Lorenzo Cotino Hueso
Presidente de la Agencia Española de Protección de Datos

>>

SEGUNDO**:** En fecha 30 de enero de 2026, ***DÉCIMAS*** ha procedido al pago de la sanción en la cuantía de **120.000,00 euros** haciendo uso de las dos reducciones previstas en el acuerdo de inicio transcrito anteriormente, lo que implica el reconocimiento de la responsabilidad en relación con los hechos a los que se refiere el acuerdo de inicio y su calificación jurídica.

TERCERO: En el acuerdo de inicio transcrito anteriormente se señalaba que, de confirmarse la infracción, podría acordarse imponer al responsable la adopción de medidas adecuadas para ajustar su actuación a la normativa mencionada en este acto, de acuerdo con lo establecido en el citado artículo 58.2 d) del RGPD, según el cual cada autoridad de control podrá *"ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado…".*

Habiéndose reconocido la responsabilidad de la infracción, procede la imposición de las medidas incluidas en el acuerdo de inicio.

FUNDAMENTOS DE DERECHO

I
Competencia

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

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

II
Terminación del procedimiento

El artículo 85 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo, LPACAP), bajo la rúbrica "*Terminación en los procedimientos sancionadores*" dispone lo siguiente:

"1. Iniciado un procedimiento sancionador, si el infractor reconoce su responsabilidad, se podrá resolver el procedimiento con la imposición de la sanción que proceda.

2. Cuando la sanción tenga únicamente carácter pecuniario o bien quepa imponer una sanción pecuniaria y otra de carácter no pecuniario pero se ha justificado la improcedencia de la segunda, el pago voluntario por el presunto responsable, en cualquier momento anterior a la resolución, implicará la terminación del procedimiento, salvo en lo relativo a la reposición de la situación alterada o a la determinación de la indemnización por los daños y perjuicios causados por la comisión de la infracción.

3. En ambos casos, cuando la sanción tenga únicamente carácter pecuniario, el órgano competente para resolver el procedimiento aplicará reducciones de, al menos, el 20 % sobre el importe de la sanción propuesta, siendo éstos acumulables entre sí. Las citadas reducciones, deberán estar determinadas en la notificación de iniciación del procedimiento y su efectividad estará condicionada al desistimiento o renuncia de cualquier acción o recurso en vía administrativa contra la sanción.

El porcentaje de reducción previsto en este apartado podrá ser incrementado reglamentariamente."

III
Pago voluntario y reconocimiento de responsabilidad

De conformidad con lo dispuesto en el citado artículo 85 de la LPACAP, en el acuerdo de inicio notificado se informaba sobre la posibilidad de reconocer la responsabilidad y de realizar el pago voluntario de la sanción propuesta, lo que supondría dos reducciones acumulables de un 20% cada una. Con la aplicación de estas dos reducciones, la sanción quedaría establecida en **120.000,00 euros** y su pago implicaría la terminación del procedimiento, sin perjuicio de la imposición de las medidas correspondientes.

Tras la notificación del citado acuerdo de inicio, ***DÉCIMAS*** ha procedido al reconocimiento de la responsabilidad y al pago voluntario de la sanción, acogiéndose a las dos reducciones previstas. De conformidad con el apartado 3 del artículo 85 LPACAP, la efectividad de las citadas reducciones estará condicionada al desistimiento o renuncia de cualquier acción o recurso en vía administrativa contra la sanción.

Debe tenerse en cuenta que, de acuerdo con los preceptos de la LPACAP, así como de la jurisprudencia del Tribunal Supremo en esta materia, el ejercicio del pago voluntario por el presunto responsable no exime a la administración de la obligación de resolver y notificar todos los procedimientos, cualquiera que sea su forma de iniciación. De igual forma, el artículo 88 de la citada norma establece que la resolución que ponga fin al procedimiento decidirá todas las cuestiones planteadas por los interesados y aquellas otras derivadas del mismo.

Por lo tanto, de acuerdo con la legislación aplicable y valorados los criterios de graduación de las sanciones, la Presidencia de la Agencia Española de Protección de Datos RESUELVE**:**

PRIMERO: DECLARAR la comisión de las infracciones y CONFIRMAR las sanciones determinadas en la parte dispositiva del acuerdo de inicio transcrito en la presente resolución.

La suma de las citadas cuantías arroja una cantidad total de **200.000,00 euros.**

Tras haber procedido ***DÉCIMAS, S.L.*** al pronto pago y reconocimiento de responsabilidad, se procede, en virtud del artículo 85 de la LPACAP, a la reducción de un 40% del total mencionado, lo cual supone la cantidad definitiva de **120.000,00 euros**.

La efectividad de las citadas reducciones está condicionada, en todo caso, al desistimiento o renuncia de cualquier acción o recurso en vía administrativa.

SEGUNDO: DECLARAR la terminación del procedimiento **EXP202408867**, de conformidad con lo establecido en el artículo 85 de la LPACAP.

TERCERO: ORDENAR a ***DÉCIMAS, S.L.*** para que en el plazo de 6 meses desde que la presente resolución sea firme y ejecutiva, notifique a la Agencia la adopción de las medidas que se describen en los fundamentos de derecho del acuerdo de inicio transcrito en la presente resolución.

CUARTO: NOTIFICAR la presente resolución a ***DÉCIMAS, S.L.***.

QUINTO: De acuerdo con lo previsto en el artículo 85 de la LPACAP que condiciona la reducción por pago voluntario y reconocimiento de la responsabilidad al desistimiento o renuncia de cualquier acción o recurso en vía administrativa, la presente resolución será firme en vía administrativa y plenamente ejecutiva a partir de su notificación.

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

Contra esta resolución, que pone fin a la vía administrativa según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, los interesados podrán interponer 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.

No obstante, conforme a lo previsto en el artículo 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://sedeaepd.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.

1259-101025

Lorenzo Cotino Hueso
Presidente de la Agencia Española de Protección de Datos