

- **Expediente N.º: EXP202209485**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: D. **A.A.A.** (en adelante, la parte reclamante) con fecha 20 de julio de 2022 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra SERVICIO DE SALUD DE CASTILLA-LA MANCHA con NIF Q4500146H (en adelante, SESCOAM). Los motivos en que basa la reclamación son los siguientes:

A principios del año 2019 el SESCOAM incoó un expediente disciplinario a la parte reclamante.

El 21 de abril de 2022 se remitió desde la dirección electrónica corporativa *****EMAIL.1** un correo electrónico a todos los profesionales que prestan servicios en la Gerencia de Urgencias, Emergencias y Transporte Sanitario (G.U.E.T.S), adjuntando, para su conocimiento, la resolución del expediente disciplinario incoado contra la parte reclamante.

La parte reclamante manifiesta que la resolución enviada no se encuentra anonimizada totalmente; puesto que, contiene referencias que permiten su identificación, prueba de ello es que recibió correos electrónicos de compañeros que habían recibido la resolución y le habían identificado. En este sentido, destaca que en la página 5 de la resolución remitida se hace una mención al domicilio del expedientado que claramente le identifica; ya que, es el único médico de la G.U.E.T.S. que tiene su residencia en la Comunidad de Canaria (conociendo sus compañeros esta circunstancia por su excepcionalidad).

Asimismo, se afirma por la parte reclamante que en la página 9 de dicha resolución se hace referencia al dato de que en esa fecha era la festividad patronal en la localidad donde presta el servicio, lo cual permite, sobre todo al personal que trabaja en la Comunidad de Castilla La Mancha, conocer perfectamente que la localidad en cuestión era Molina de Aragón, la cual celebra sus fiestas patronales entre el 29 y el 3 de septiembre.

Junto a la reclamación aporta el correo remitido por la parte reclamada al que se adjuntó la resolución del expediente sancionador, seis correos electrónicos remitidos por los compañeros a la parte reclamante para comentarle lo sucedido y la resolución anexada al correo controvertido.

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 al SESCOAM, para que procediese a su análisis e informase a esta Agencia en el plazo de un mes, de las acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos.

El traslado, 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 recogido en fecha 15 de septiembre de 2022 como consta en el certificado que obra en el expediente.

Con fecha 18 de octubre de ese mismo año se recibe en esta Agencia escrito de respuesta indicando que *“...Al reclamante, trabajador de la Gerencia de Urgencias y Emergencias de SESCOAM, le fue abierto expediente disciplinario por unos hechos de gravedad y gran repercusión en el funcionamiento y la organización de la Gerencia de Urgencias y Emergencias.*

Dictada la correspondiente resolución en la que se procedía a sancionar a dicho trabajador, la Gerencia retiró todos los datos de carácter personal de la misma a fin de remitirla, de forma anonimizada, al resto de trabajadores de la misma con el fin de que dichos comportamientos no prosperasen y evitar así la apertura de otros expedientes disciplinarios en los que pudiesen verse perjudicados otros trabajadores de la Gerencia...Dicha Resolución fue anonimizada correctamente, sin que de los datos que constan en la Resolución que se envió se dedujese la identidad de la persona a la que se refiere.

No constaban en la resolución enviada el nombre y apellidos del trabajador, ni centro de trabajo en el que estaba ubicado, ni el área geográfica en el que se ubicaba. Tampoco se identificaba a la persona con iniciales, ni constaba domicilio, ni DNI. En definitiva, no solo no constaba el nombre de la persona a la que se refería la Resolución, ni ningún otro dato de carácter personal que identificara a la persona que había sido sancionada. No constaba ni el lugar en el que trabajaba, ni ningún dato que revelase la identidad de la persona a la que se refería la Resolución...”.

TERCERO: Con fecha 20 de octubre de 2022, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la parte reclamante.

CUARTO: Con fecha 23 de noviembre de 2022, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la parte reclamada, por la presunta infracción del artículo 5.1.f) del RGPD y artículo 32 del RGPD, tipificadas en el artículo 83.5 del RGPD y el artículo 83.4 del RGPD, respectivamente.

QUINTO: Notificado el citado acuerdo de inicio 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), con fecha 13 de diciembre de 2002 se recibió en la Agencia Española de Protección de Datos escrito comunicando la intención de no hacer alegaciones al acuerdo de inicio notificado.

El artículo 64.2.f) de la LPACAP -disposición de la que se informó a la parte reclamada en el acuerdo de apertura del procedimiento- establece que si no se efectúan alegaciones en el plazo previsto sobre el contenido del acuerdo de iniciación, cuando

éste contenga un pronunciamiento preciso acerca de la responsabilidad imputada, podrá ser considerado propuesta de resolución. En el presente caso, el acuerdo de inicio del expediente sancionador determinaba los hechos en los que se concretaba la imputación, la infracción del RGPD atribuida a la reclamada y la sanción que podría imponerse. Por ello, tomando en consideración que la parte reclamada no ha formulado alegaciones al acuerdo de inicio del expediente y en atención a lo establecido en el artículo 64.2.f) de la LPACAP, el citado acuerdo de inicio es considerado en el presente caso propuesta de resolución.

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

HECHOS PROBADOS

PRIMERO: Ha quedado acreditado que el día 21 de abril de 2022 se remitió desde la dirección electrónica corporativa *****EMAIL.1** un correo electrónico a todos los profesionales que prestan servicios en la Gerencia de Urgencias, Emergencias y Transporte Sanitario (G.U.E.T.S), adjuntando, para su conocimiento, la resolución del expediente disciplinario incoado contra la parte reclamante.

SEGUNDO: Ha quedado acreditado que la resolución enviada no se encontraba anonimizada totalmente, conteniendo referencias que permitían la identificación de la parte reclamante.

FUNDAMENTOS DE DERECHO

I

De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada autoridad de control y según lo establecido en los artículos 47, 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 Directora de la Agencia Española de Protección de Datos.

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

II

Artículo 5.1.f) del RGPD

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

"1. Los datos personales serán:

(...)

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

En el presente caso, consta que los datos personales de la parte reclamante, obrantes en la base de datos del SESCOAM, fueron indebidamente difundidos al resto de profesionales que prestan servicios en la Gerencia de Urgencias, Emergencias y Transporte Sanitario (G.U.E.T.S), vulnerándose el principio de confidencialidad.

Desde la dirección electrónica corporativa *****EMAIL.1** se envió un correo electrónico a todos los profesionales que prestan servicios en la Gerencia de Urgencias, Emergencias y Transporte Sanitario (G.U.E.T.S), adjuntando, para su conocimiento, la resolución del expediente disciplinario incoado contra la parte reclamante.

Dicha resolución no se encuentra anonimizada totalmente, conteniendo referencias que permiten la identificación de la parte reclamante.

En este sentido, debemos recordar la definición de dato personal contenido en la artículo 4 del RGPD: “... «datos personales»: 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...”.

Sin olvidar que, en el considerando 26 del mismo texto legal se dispone que los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable.

III

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

La citada infracción del artículo 5.1.f) del RGPD supone la comisión de las infracciones tipificadas en el artículo 83.5 del RGPD que bajo la rúbrica “*Condiciones generales para la imposición de multas administrativas*” dispone:

“Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

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

A este respecto, la LOPDGDD, en su artículo 71 “*Infracciones*” establece que:

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

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

“1. En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

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

IV

Sanción por la infracción del artículo 5.1.f) del RGPD

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

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

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

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

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

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

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

Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que

no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda.

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

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

V

Artículo 32 del RGPD

El Artículo 32 “Seguridad del tratamiento” del RGPD establece:

“1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

- a) la seudonimización y el cifrado de datos personales;*
- b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;*
- c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;*
- d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.*

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

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

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

En el presente caso, en el momento de producirse la brecha de seguridad, no consta que el SESCOAM dispusiese de medidas de seguridad razonables en función de los posibles riesgos estimados.

El SESCOAM manifiesta que *“La Resolución enviada a todos los trabajadores fue revisada por 3 personas a fin de eliminar los datos de carácter personal existentes. La Resolución pasó 3 filtros antes de ser enviada: la primera persona que realizó la anonimización, el superior inmediato que lo revisó y por último, la Dirección de Gestión que procedió a su revisión antes de su envío.”*

Dicha manifestación deja en evidencia el desconocimiento del personal que ha intervenido en el proceso en relación con la anonimización de los datos.

En este sentido es importante resaltar que los datos se considerarán anonimizados en la medida que no exista una probabilidad razonable de que cualquier persona pueda identificar a la persona física en el conjunto de datos.

Con el proceso de anonimización se pretenden eliminar o reducir al mínimo los riesgos de reidentificación de los titulares de los datos, pero sin distorsionar el tratamiento de datos.

La finalidad es ofrecer mayores garantías de privacidad a las personas, impidiendo la vulneración de la confidencialidad, integridad y disponibilidad de los sistemas y servicios de tratamiento.

En el presente caso, los datos personales de la parte reclamante que figuran en la resolución adjuntada al correo electrónico enviado, no se encuentran correctamente anonimizados permitiendo que la parte reclamante puede ser identificable para personas que conozcan las circunstancias no anonimizadas, particularmente su lugar de residencia, dado lo peculiar de este último.

Por lo demás, la manera de actuar del personal, tal y como está descrita, comporta un alto riesgo de que errores como este puedan producirse.

El SESCOAM no ha aportado a este procedimiento ningún documento sobre instrucciones o formación a su personal en relación con determinadas prácticas, como esta, que comportan un riesgo de producción de una brecha de seguridad que afecte a los datos personales.

Es más, en relación con las medidas que piensa adoptar para que no se vuelva a producir un incidente similar en el futuro, el reclamado manifiesta que *“...las medidas a adoptar son las que se han adoptado hasta la fecha: Que la documentación pase los filtros necesarios para detectar que no quede ningún dato de carácter personal, considerado SENSIBLE...”* considerando *“...la posibilidad de adquirir un programa informático específico para facilitar esta anonimización de datos...”* resaltando que el mismo sería *“... únicamente para facilitar su labor a las personas que llevan a cabo esta anonimización...”* sin plantear; en ningún caso, la necesidad de profundizar en la formación de su personal en relación con los procesos y herramientas de anonimización, para que incidentes como el ocurrido no vuelvan a repetirse en el futuro.

VI

Tipificación de la infracción del artículo 32 del RGPD

La citada infracción del artículo 32 del RGPD supone la comisión de las infracciones tipificadas en el artículo 83.4 del RGPD que bajo la rúbrica “*Condiciones generales para la imposición de multas administrativas*” dispone:

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

- 5) *las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43; (...)*”

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

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

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

...

- f) *La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679. (...)*”.

VII

Sanción por la infracción del artículo 32 del RGPD

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

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

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

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

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

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

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

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

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

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

VIII Medidas

El artículo 58.2 del RGPD dispone: “Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:

d) 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...”.

Asimismo, procede imponer la medida correctiva descrita en el artículo 58.2.d) del RGPD y ordenar al SESCOG que, en el plazo de tres meses, establezca las medidas de seguridad adecuadas para que se adecúen los tratamientos a las exigencias contempladas en los artículos 5.1 f) y 32 del RGPD, impidiendo que se produzcan situaciones similares en el futuro.

En el texto de la resolución se establecen cuáles han sido las infracciones cometidas y los hechos que han dado lugar a la vulneración de la normativa de protección de datos, de lo que se infiere con claridad cuáles son las medidas a adoptar, sin perjuicio

de que el tipo de procedimientos, mecanismos o instrumentos concretos para implementarlas corresponda a la parte sancionada, pues es el responsable del tratamiento quien conoce plenamente su organización y ha de decidir, en base a la responsabilidad proactiva y en enfoque de riesgos, cómo cumplir con el RGPD y la LOPDGDD, informando de todo ello a este organismo.

Por lo tanto, de acuerdo con la legislación aplicable y valorados los criterios de graduación de las sanciones cuya existencia ha quedado acreditada, la Directora de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: IMPONER al SERVICIO DE SALUD DE CASTILLA-LA MANCHA, con NIF Q4500146H, por una infracción del Artículo 5.1.f) del RGPD, tipificada en el artículo 83.5 del RGPD, una sanción de apercibimiento.

IMPONER al SERVICIO DE SALUD DE CASTILLA-LA MANCHA, con NIF e, por una infracción del Artículo 32 del RGPD, tipificada en el artículo 83.4 del RGPD, una sanción de apercibimiento.

SEGUNDO: REQUERIR al SERVICIO DE SALUD DE CASTILLA-LA MANCHA, que implante, en el plazo de tres meses, las medidas correctoras necesarias para adecuar su actuación a la normativa de protección de datos personales, que impidan que en el futuro se repitan hechos similares, así como que informe a esta Agencia en el mismo plazo sobre las medidas adoptadas.

TERCERO: NOTIFICAR la presente resolución a SERVICIO DE SALUD DE CASTILLA-LA MANCHA.

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

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

Contra esta resolución, que pone fin a la vía administrativa conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) de la LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la Agencia Española de Protección de Datos, presentándolo a través

del Registro Electrónico de la Agencia [<https://sedeagpd.gob.es/sede-electronica-web/>], o a través de alguno de los restantes registros previstos en el art. 16.4 de la citada Ley 39/2015, de 1 de octubre. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

938-181022

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