

- Expediente Nº: PS/00365/2021

### RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

#### ANTECEDENTES

PRIMERO: Dña. **A.A.A.** (en adelante la reclamante) con fecha 18/06/2020 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra SERVICIO CANTABRO DE SALUD con CIF S3933002B (en adelante, el SCS ó el reclamado). Los motivos en que basa la reclamación son que han mezclado sus datos de salud y los de otra persona que tiene el mismo nombre y apellidos, pero distinto DNI. Lo ha puesto en conocimiento del SCS en distintas ocasiones a través de escritos para que se corrija el error, con resultado infructuoso.

Y aporta la siguiente documentación;

- Copia de correo electrónico de fecha 16/11/2019 remitido por **\*\*\*EMAIL.1** y enviado a **\*\*\*EMAIL.2** donde constan el nombre y apellidos de la reclamante junto al correo electrónico remitente y el sello del SCS con fecha 25/11/2019. En dicho correo electrónico se manifiesta que sus datos han sido mezclados con los de otra persona que tiene su nombre y apellidos iguales a los suyos. Que este problema lo detectó por primera vez en el año 2012.

- Copia de correo electrónico de fecha 04/12/2019 remitido por **\*\*\*EMAIL.1** y enviado a **\*\*\*EMAIL.2** donde constan el nombre y apellidos de la reclamante junto al correo electrónico remitente y el sello del SCS con fecha 19/12/2019. En dicho correo electrónico se manifiesta que en el Centro de Salud de **\*\*\*LOCALIDAD.1** en fecha 29/11/2019, tras entregar su DNI, quien le atendió vio en su pantalla que en sus datos no se correspondía el DNI con el auténtico, que los primeros números eran los mismos y los últimos y la letra era diferente.

- Copia de reclamación presentada en fecha 10/01/2020 al reclamado.

Posteriormente, en julio de 2020 le comunican que la situación se había resuelto; no obstante, llamó al Centro de Salud de **\*\*\*LOCALIDAD.1** a fin de solicitar cita previa para la vacuna de la gripe, ya que siempre se ha vacunado allí y le informan que tenía que vacunarse en el Centro de Salud de Santander donde estaba inscrita. Que después de dar su DNI en el Centro de Salud de **\*\*\*LOCALIDAD.1**, se constató que no existe referencia a su persona ni aparece ningún dato suyo.

Y aporta copia de certificado del SCS (Gerencia de Atención Primaria) fechado y firmado a 01/07/2020, donde se manifiesta que, tras detectar el error, se ha procedido a subsanar el mismo respecto de los datos administrativos de la reclamante. Consta en el certificado el nombre y dos apellidos de la reclamante, así como los dígitos tercero, cuarto, quinto, sexto de su DNI así como la letra.

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), con número de referencia E/05273/2020, se dio traslado de dicha reclamación al reclamado el 26 de junio de 2020, 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.

TERCERO: Con fecha 16/10/2020, la Directora de la AEPD acuerda la admisión a trámite de la reclamación.

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

Con fecha 03/03/2021 se envía requerimiento de información al reclamado. La notificación se realiza electrónicamente a través de *notific@*. La notificación consta entregada con fecha 04/03/2021. No se recibe contestación.

QUINTO: Con fecha 12/08/2021, la Directora de la Agencia Española de Protección de Datos acordó iniciar, procedimiento sancionador al reclamado por la presunta infracción de los artículos 5.1.f) y 32.1 del RGPD, sancionada conforme a lo dispuesto en los artículos 83.5.a) y 83.4.a) del citado RGPD, considerando que la sanción que pudiera corresponderle sería de apercibimiento.

SEXTO: Notificado el acuerdo de inicio, el reclamado presentó escrito de alegaciones el 23/08/2021 en el que manifiesta, en síntesis, lo siguiente: que no tiene constancia de haber recibido la documentación de fecha 26/06/2021; que en todo momento se ha procurado analizar y solventar los hechos y circunstancias planteadas por la persona interesada, incidiendo en la necesaria seguridad y confidencialidad de sus datos personales; que la persona interesada requirió a este SCS en ejercicio de su derecho de rectificación de datos personales, habiéndola dado respuesta mediante resolución desestimatoria e informando de la necesaria preservación de sus datos con el objeto de adecuarlos a la asistencia sanitaria que pudiera precisarse; que se han adoptado las medidas precisas y facilitado la comunicación con la persona interesada en todo momento.

SEPTIMO: Con fecha 13/10/2021 se inició el período de práctica de pruebas, acordándose las siguientes:

Dar por reproducidos a efectos probatorios la reclamación interpuesta por la reclamante y su documentación, los documentos obtenidos y generados que forman parte del procedimiento E/08372/2020.

Dar por reproducido a efectos probatorios, las alegaciones al acuerdo de inicio del procedimiento sancionador referenciado, presentadas por el reclamado y la

documentación que a ellas acompaña.

OCTAVO: El 16/11/2020 fue notificada Propuesta de Resolución en el sentido de que por la Directora de la AEPD se sancionara al reclamado por infracción de los artículos 5.1.f) y 32.1 del RGPD, tipificadas en los artículos 83.5.a) y 83.4.a) del RGPD, con apercibimiento.

Transcurrido el plazo establecido el reclamado, al tiempo de la presente Resolución, no había presentado escrito de alegación alguno.

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

#### HECHOS PROBADOS

PRIMERO. El 18/06/2020 la reclamante interpuso reclamación ante la AEPD contra el reclamado, manifestado que se han mezclado sus datos de salud y los de otra persona que tiene el mismo nombre y apellidos, pero distinto DNI y que puesto en conocimiento en distintas ocasiones a través de escritos para que se corrija el error, el resultado ha sido infructuoso.

SEGUNDO. La reclamante ha aportado copias de los correos electrónicos de fecha 16/11/2019 y 04/12/2019 dirigidos al reclamado; en el primero le solicita la protección de sus datos de carácter personal que habían sido mezclados con los de otra persona con sus mismos nombre y apellidos situación que arrastra a desde 2012 y, en el segundo, manifiesta que en el Centro de Salud de **\*\*\*LOCALIDAD.1** en fecha 29/11/2019, tras entregar su DNI, quien le atendió vio en su pantalla que en sus datos no se correspondía el DNI con el auténtico, que los primeros números eran los mismos y los últimos y la letra era diferente.

TERCERO. La reclamante aporta copia de reclamación presentada en fecha 10/01/2020 ante la ausencia de respuestas a los correos remitidos y anomalías observadas en relación con sus datos.

CUARTO. La afectada dirigió al reclamado nuevo escrito de reclamación el 16/06/2020 al no haber recibido ninguna respuesta a los escritos remitidos con anterioridad así como la desatención y desinterés hacia su problema.

QUINTO. El reclamado en escrito de 19/07/2021 ha señalado que: *“Se detectó error en la documentación clínica de carácter pasivo obrante en la Gerencia de Atención Primaria que pertenece a la reclamante en relación al episodio clínico referido al Centro de Salud de **\*\*\*LOCALIDAD.2** y que se encontraba registrado en la Historia clínica de D<sup>a</sup>. **A.A.A.**, con DNI **\*\*\*NIF.1** del Centro de Salud de **\*\*\*LOCALIDAD.3** en Santander”*.

SEXTO. El reclamado ha aportado documentación clínica de carácter pasivo obrante en la Gerencia de Atención Primaria perteneciente a la reclamante, en su condición de usuaria de MUFACE que consta en el histórico de AP Cantabria, así como de D<sup>a</sup>. **A.A.A.**, con DNI **\*\*\*NIF.1**, en su condición de usuaria del Servicio Público de Salud de la Comunidad de Cantabria.

SEPTIMO. El reclamado ha aportado certificación, de 01/07/2020, de La Directora Ge-

rente de La Gerencia de Atención Primaria, responsable del tratamiento de los datos relativos a la salud de todos los usuarios activos e inactivos de la Comunidad Autónoma de Cantabria a través de la aplicación Visor Corporativo del Servicio Cántabro de Salud, de que había procedido a subsanar el error detectado respecto de los datos administrativos de la reclamante, en su condición de usuaria de MUFACE.

OCTAVO. El reclamado ha manifestado que desde la Dirección Gerencia del SCS se solicitó la rectificación en datos de carácter personal y de orden administrativo de la ficha activa de la tercera persona en el C.S. Lardo y así se procedió a la fusión con la ficha del histórico de la reclamante. Y aporta escrito de la Coordinadora de Sistemas de Información de la GAP, que señala:

*“26/06/2020*

*Se han rectificado los datos administrativos de la ficha activa de D<sup>a</sup>. A.A.A., con DNI \*\*\*NIF.1, en \*\*\*LOCALIDAD.2 y así se ha procedido a la fusión con la ficha del histórico de la reclamante.*

*De esta forma queda una única historia clínica la reclamante en el histórico de OMI de C.S. de \*\*\*LOCALIDAD.2.*

NOVENO. Consta oficio de la Gerencia de Atención Primaria de fecha 01/07/2020 dirigido a la reclamante, asunto rectificación de datos personales administrativos de usuaria Muface, en la que se señala:

*“En relación a su solicitud para que se proceda a efectuar RECTIFICACIÓN en datos de carácter personal y de orden administrativo en la documentación clínica de carácter pasivo y que obra en la Gerencia de Atención Primaria, adjunto le remito certificación correspondiente a la rectificación operada según verificación previa por la Coordinadora del Servicio de Sistemas de información de esta institución sanitaria. Lo que se comunica a los efectos correspondientes”.*

## FUNDAMENTOS DE DERECHO

### I

En virtud de los poderes que el artículo 58.2 del RGPD reconoce a cada autoridad de control, y según lo establecido en los artículos 47 y 48 de la LOPDGDD, la Directora de la Agencia Española de Protección de Datos es competente para iniciar y para resolver este procedimiento.

### II

El artículo 5 del RGPD establece los principios que han de regir el tratamiento de los datos personales y menciona entre ellos el de “integridad y confidencialidad”.

El citado artículo señala que:

*“1. Los datos personales serán:*

*(...)*

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

*(...)*

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

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

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

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

### III

La documentación obrante en el expediente ofrece indicios evidentes de que el reclamado, vulneró el artículo 5 del RGPD, *principios relativos al tratamiento*, en relación con el artículo 5 de la LOPDGDD, *deber de confidencialidad*, al combinar y mezclar los datos de salud de la reclamante con los de un tercero con el mismo nombre y apellidos pero distinto DNI.

Considera la reclamante que la combinación de sus datos de salud con los de una tercera persona que tiene su mismo nombre y apellidos, pero distinto DNI, y la posibilidad de que los datos sean conocidos por sus respectivos titulares o terceros, supone una vulneración del deber de confidencialidad, contemplado en el artículo 5.1.f) del RGPD, así como del artículo 5 de la LO 3/2018, de 5 de diciembre, de Protección de datos personales y garantía de los derechos digitales.

Artículo 5 de la Ley Orgánica 3/2018, de 5 de diciembre, a cuyo tenor: *“ los responsables y encargados de tratamiento de datos así como todas las personas que intervengan en cualquier fase de este estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1.f) del reglamento (UE) 2016/679.*

Estableciendo a su vez el artículo 5.1.f) del referido RGPD que: *“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».*

Deber de confidencialidad o secreto, que constituye una de las manifestaciones esenciales del derecho fundamental de protección de datos personales ( artículo 18.4 CE), y que en el presente supuesto ha sido vulnerado como manifiesta el propio reclamado cuando señala todo fue debido a un error humano, error que posibilita el acceso no autorizado a los datos y que sean conocidos por terceros, al no ser identificados correctamente mediante su DNI: *“Se detectó error en la documentación clínica de carácter pasivo obrante en la Gerencia de Atención Primaria que pertenece a la reclamante en relación al episodio clínico referido al Centro de Salud de \*\*\*LOCALIDAD.2 y que se encontraba registrado en la Historia clínica de D<sup>a</sup>. A.A.A., con DNI \*\*\*NIF.1 del Centro de Salud de \*\*\*LOCALIDAD.3 en Santander”.*

Además, ha indicado que *“La Directora Gerente de La Gerencia de Atención Primaria, responsable del tratamiento de los datos relativos a la salud de todos los*



*usuarios activos e inactivos de la Comunidad Autónoma de Cantabria a través de la aplicación Visor Corporativo del Servicio Cántabro de Salud, había procedido a subsanar el error detectado respecto de los datos administrativos de la reclamante, en su condición de usuaria de MUFACE”.*

#### IV

El artículo 83.5 a) del RGPD, considera que la infracción de *“los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9”* es sancionable.

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

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

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

#### V

En segundo lugar, hay que señalar que la seguridad de los datos personales viene regulada en los artículos 32, 33 y 34 del RGPD.

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

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

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

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

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

*4. El responsable y el encargado del tratamiento tomarán medidas para garan-*

*tizar 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”.*

## VI

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

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

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

*(...)”*

Por su parte, la LOPDGDD en su artículo 73, a efectos de prescripción, califica de “Infracciones consideradas graves:

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

*(...) ”*

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

*(...)”*

Los hechos puestos de manifiesto en la presente reclamación se concretan en el incumplimiento de las medidas técnicas y organizativas establecidas vulnerando la confidencialidad de los datos al combinar los datos de salud de la reclamante con los de una tercera persona con el mismo nombre y apellidos, pero distinto DNI.

## VII

En lo que se refiere a las medidas de seguridad, el RGPD establece en su artículo 5.1.f) como uno de los principios en materia de protección de datos el del tratamiento de los datos con una seguridad adecuada, lo que significa que se deben aplicar las medidas técnicas y organizativas que sean adecuadas para protegerse contra el tratamiento no autorizado o ilícito y de la pérdida, destrucción y daño accidental de los datos.

El artículo 32 del RGPD establece que hay que aplicar medidas técnicas y organizativas teniendo en cuenta el estado de la técnica, los costes de aplicación de las medidas, la naturaleza, alcance, contexto y finalidades del tratamiento; los riesgos de probabilidad y gravedad para los derechos y libertades de las personas interesadas.

En relación con esto último, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales: destrucción, pérdida o alteración accidental o ilícita de datos personales, comunicación o acceso no autorizados a dichos datos,

y que pudieran ocasionar daños y perjuicios físicos, materiales o inmateriales. (El Considerando 83 del RGPD es muy esclarecedor en este aspecto).

Entre estas medidas se encuentran: la seudonimización y el cifrado, la capacidad para garantizar la confidencialidad, integridad, disponibilidad y resiliencia, la capacidad para restaurar la disponibilidad y acceso a datos tras un incidente, proceso de verificación (que no auditoría), evaluación y valoración de la eficacia de las medidas.

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

*“(83) A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales”.*

En el presente caso, tal y como consta en los hechos y en la documentación que integra el expediente de investigación E/05273/2020, la AEPD trasladó al reclamado el 26/06/2020 la reclamación presentada para su análisis solicitando la aportación de información relacionada con la incidencia reclamada y sin que conste la respuesta del reclamado.

Sobre este cuestión señala el reclamado que, en caso de haberse recibido la documentación, se le habría dado curso como a los demás escritos y comunicaciones que se reciben, no así del escrito de 26/06/2020, nunca recibido en dicha gerencia.

No obstante, la responsabilidad del reclamado viene determinada por el incidente de seguridad puesta de manifiesto por la reclamante, ya que es responsable de tomar decisiones destinadas a implementar de manera efectiva las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo para asegurar la confidencialidad de los datos, restaurando su disponibilidad e impedir el acceso a los mismos en caso de incidente físico o técnico.

De la documentación aportada se desprende que la entidad incumplió esta obligación, debido al error cometido en la documentación del reclamante al combinarla con la de un tercero usuario igualmente de los servicios de salud en el momento de su identificación inequívoca. Como ya se señalaba en fundamento anterior el reclamado mediante escrito de 19/07/2021 indicaba que: *“Se detectó error en la documentación clínica de carácter pasivo obrante en la Gerencia de Atención Primaria que pertenece a la reclamante en relación al episodio clínico referido al Centro de Salud de **\*\*\*LOCALIDAD.2** y que se encontraba registrado en la Historia clínica de D<sup>a</sup>. **A.A.A.**, con DNI **\*\*\*NIF.1** del Centro de Salud de **\*\*\*LOCALIDAD.3** en Santander”.*



No obstante, como señala el reclamado *“Desde Dirección Gerencia del SCS se solicita la rectificación de datos de carácter personal y de orden ...”* y que *“se había procedido a subsanar el error detectado respecto de los datos administrativos de la reclamante, en su condición de usuaria de MUFACE”*.

Por tanto, se estima que el reclamado vulneró el artículo 32 del RGPD, infracción tipificada en su artículo 83.4.a).

## VIII

Hay que señalar que la LOPDGDD en su artículo 77, *Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento*, establece lo siguiente:

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

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

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

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

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

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

da.

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

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

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

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

De conformidad con las evidencias de las que se dispone dicha conducta constituye, por parte del reclamado la infracción a lo dispuesto en los artículos 5.1.f) y 32.1 del RGPD.

El RGPD, sin perjuicio de lo establecido en su artículo 83, contempla en su artículo 77 la posibilidad de acudir a la sanción de apercibimiento para corregir los tratamientos de datos personales que no se adecúen a sus previsiones, 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.

En el presente caso, el reclamado a través de la Dirección Gerencia del SCS solicitó la rectificación de los datos de carácter personal y de orden administrativo de la reclamante, aportando certificación de la Gerencia de Atención Primaria, responsable del tratamiento de los datos relativos a la salud de todos los usuarios activos e inactivos de la Comunidad Autónoma de Cantabria en la que señalaba que se había procedido a subsanar el error detectado respecto de los datos administrativos de aquella, en su condición de usuaria de MUFACE. También consta escrito dirigido a la reclamante comunicándole la rectificación llevada a cabo en la documentación clínica de carácter pasivo.

Por último ha señalado que para evitar incidencias como la que dio lugar a la reclamación se activaran alertas a los profesionales sanitarios que accedan a la documentación clínica de pacientes para que revisen la identidad exacta de cada paciente o usuario en el momento del acceso, para evitar errores humanos.

Por tanto, no procede instar la adopción de medidas adicionales, al haber adoptado medidas razonables, de conformidad con la normativa en materia de protección de datos, que es la finalidad principal de los procedimientos respecto de aquellas entidades relacionadas en el artículo 77 de la LOPDGDD.

Por todo ello, 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 CANTABRO DE SALUD, con CIF Q3900738J, por una infracción de los artículos 5.1.f) y 32.1 del RGPD, tipificados en los artículos 83.5.a) y 83.4.g) del RGPD, una sanción de *apercibimiento*.

SEGUNDO: NOTIFICAR la presente resolución a SERVICIO CANTABRO DE SALUD, con CIF Q3900738J.

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

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

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) de la LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la Agencia Española de Protección de Datos, presentándolo a través del Registro Electrónico de la Agencia [<https://sedeagpd.gob.es/sede-electronica-web/>], o a través de alguno de los restantes registros previstos en el art. 16.4 de la citada Ley 39/2015, de 1 de octubre. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

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