- Expediente Nº: PS/00473/2021

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

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

HECHOS

PRIMERO: D. ***A.A.A.*** (en adelante, la parte reclamante) con fecha 19/08/2020 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra la CONSEJERÍA DE SANIDAD de la C.C.A.A. de MADRID, con CIF S7800001E (en adelante, la parte reclamada). Los motivos en que basa la reclamación son los siguientes: el reclamante manifiesta que un tercero ha utilizado su identidad para cambiar su adscripción a otro Centro de Salud y que interpuestas denuncias policiales se ha dado nueva cita a la persona que usurpó su identidad.
Y aporta:

- Documento de "*Relación de citas pendientes"* fechado a 05/08/2020 donde consta el nombre y apellidos del reclamante, en *"fecha de nacimiento"* consta "26/11/1988" y constan dos citas en el mes de agosto de 2020.
- Documento de *"Relación de problemas de salud*" fechado a 05/08/2020 donde consta el nombre y apellidos del reclamante, en "f*echa de nacimiento*" consta "26/11/1988".
- Documento de "*Relación de citas pendientes*" fechado a 18/08/2020 donde consta una cita para el 10/08/2020 en el Centro de Salud ******CENTRO.1***.
- Denuncia policial.

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, en el ámbito del E/10590/2020, a la parte reclamada el 08/10/2020, 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.
La entidad no ha dado respuesta al traslado de la reclamación.

TERCERO: Con fecha 21/12/2020 la Directora de la Agencia Española de Protección de Datos acordó admitir a trámite la reclamación presentada por la parte reclamante.

CUARTO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos, teniendo conocimiento de los siguientes extremos:

Con fecha 26/05/2021 se envía requerimiento de información al reclamado. La notificación se realiza electrónicamente a través de notific@. La notificación consta entregada con fecha 27/05/2021. No se recibe contestación.

QUINTO: Con fecha 6 de octubre de 2021, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la parte reclamada, por la presunta infracción del Artículo 32 del RGPD y Artículo 5.1.d) del RGPD, tipificada en el Artículo 83.4 del RGPD.

SEXTO: Con fecha 06/10/2021, 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.d) y 32.1 del RGPD, tipificadas en los artículos 83.5.a) y 83.4.a) del citado RGPD.

SEPTIMO: Notificado el acuerdo de inicio, el reclamado mediante escrito de 14/10/2021 solicito la subsanación del acuerdo de inicio; subsanación que le fue notificada mediante acuerdo de 26/10/2021.

El 15/11/2021 el reclamado presentó escrito de alegaciones manifestando en síntesis: que se había producido problemas en el registro de la oficina de internet, razón por la cual en su momento no se pudo tener conocimiento del requerimiento informativo de la AEPD; que recibido el acuerdo de inicio se solicitó su subsanación y que posteriormente ese procedió a dar respuesta inmediata a las petición de información quedando constatado que no se había producido una suplantación de personalidad en la persona del reclamante sino un error humano en la identificación de dos ciudadanos con el mismo nombre y apellidos.

OCTAVO: Con fecha 18/11/2021 se inició un período de práctica de pruebas, acordándose las siguientes;

> Dar por reproducidos a efectos probatorios la reclamación interpuesta por el reclamante y su documentación, los documentos obtenidos y generados por los Servicios de Inspección que forman parte del expediente E/10590/2020.
>
> Dar por reproducido a efectos probatorios, las alegaciones al acuerdo de inicio PS/00473/2021 presentadas por el reclamado y la documentación que a ellas acompaña.

NOVENO: El 14/02/2022 fue notificada al reclamado 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.d) 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.

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

HECHOS PROBADOS

PRIMERO. El 06/11/2020 tiene entrada en la Agencia Española de Protección de Datos escrito del afectado manifestando que a comienzos de 2020 solicitó por primera

vez su tarjeta sanitaria al centro de salud ***CENTRO.2**, ; que con fecha 05/08/2020 al solicitar cita online con su médico, solo podía solicitar cita para el centro de salud ***CENTRO.1**, C/ ***DIRECCIÓN.1**, Madrid; que llamando al centro de salud ***CENTRO.2** comprueba que su DNI está correcto pero también le indican que su domicilio está en la C/ ***DIRECCIÓN.2** (Vallecas) y el número de teléfono no es el suyo; que alguien ha cambiado sus datos, si bien para llevarlo a cabo debe cumplir con un protocolo: identificarse y aportar el certificado de empadronamiento actualizado, gestión que el centro de salud ***CENTRO.1** parece haber omitido y ha dado lugar a que otra persona suplante su identidad; que si bien nunca ha usado la sanidad pública, constan citas reservadas y un historial médico que no le corresponde; que ha interpuesto denuncias policiales, si bien no han tomado ninguna medida ni se han comunicado con él.

SEGUNDO. El reclamante ha aportado documento Relación de citas pendientes del Servicio de Atención Primara de Salud Madrid de fecha 05/08/2020, documento Relación de problemas de salud de fecha 05/08/2020 y documento Relación de citas pendientes de fecha 18/08/2020 (donde consta una cita para el 10/08/2020 en el Centro de Salud ***CENTRO.1**), relativos al tercero cuyo nombre, apellidos, coincide con el reclamante.

TERCERO. Consta aportada Denuncia ante la Policía Nacional, dependencias de Madrid-Retiro el 06/08/2020.

CUARTO. El reclamado en escrito de 10/08/2021 ha señalado que *"la incidencia producida tiene su origen en que existe otro ciudadano que coincide en nombre y apellidos con el denunciante, es decir, no se ha producido una suplantación de identidad como tal del ciudadano, sino que, por causa de un error humano en la identificación, al no seguirse los protocolos establecidos, dio lugar a la confusión producida*.

De esta forma, una vez realizadas las averiguaciones pertinentes, se ha podido concluir que, sobre la ficha administrativa del reclamante se realizó un cambio en el domicilio del mismo al haberse atendido al ciudadano con el mismo nombre y apellidos, sin haber comprobado el DNI o pasaporte del solicitante".

QUINTO. El reclamado ha aportado informe emitido el 15/09/2021 por la Gerencia Asistencial de Atención Primaria en el que se describen los hechos ocurridos y señalan las medidas de seguridad existentes y las adoptadas para evitar que se produzcan incidentes similares.

SEXTO. Consta aportada comunicación dirigida al ciudadano de 05/10/2021, donde le informan que, una vez efectuadas las investigaciones pertinentes, en el mes de septiembre del año 2020 procedieron a rectificar de oficio aquellos datos de su historia clínica e información poblacional que se registraron por error.

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

Los hechos denunciados vienen motivados por la suplantación de la identidad del reclamante por un tercero con ocasión del cambio de su adscripción a otro Centro de Salud sin que se haya dado respuesta a su reclamación.

En primer lugar, El RGPD se ocupa en su artículo 5 de los principios que han de regir el tratamiento de los datos personales y menciona entre ellos el de exactitud, señalando:

"1. Los datos personales serán:

(…)

d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);

(…)"

Lo que antecede hay que ponerlo en relación con el artículo 5, *Exactitud de los datos*, 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), que señala en su apartado 1:

"1. Conforme al artículo 5.1.d) del Reglamento (UE) 2016/679 los datos serán exactos y, si fuere necesario, actualizados

(…)"

Y el Considerando 71 del RGPD dispone que, *"(...) a fin de garantizar un tratamiento leal y transparente respecto del interesado, teniendo en cuenta las circunstancias y contexto específicos en los que se tratan los datos personales, el responsable del tratamiento debe utilizar procedimientos matemáticos o estadísticos adecuados para la elaboración de perfiles, aplicar medidas técnicas y organizativas apropiadas para garantizar, en particular, que se corrigen los factores que introducen inexactitudes en los datos personales y se reduce al máximo el riesgo de error, asegurar los datos personales de forma que se tengan en cuenta los posibles riesgos para los intereses y derechos del interesado e impedir, entre otras cosas, efectos discriminatorios en las personas físicas por motivos de raza u origen étnico, opiniones políticas, religión o creencias, afiliación sindical, condición genética o estado de salud u orientación sexual, o tratamiento que dé lugar a medidas que produzcan tal efecto".*

III

La infracción que se le atribuye a la reclamada se encuentra tipificada en el artículo 83.5 a) del RGPD, que 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, de acuerdo con el apartado 5 del mencionado artículo 83 del citado Reglamento.

La LOPDGDD en su artículo 71, *Infracciones,* señala que:

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

Y en su artículo 72, considera a efectos de prescripción, que son*: "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.

(…)".

IV

De la documentación obrante en el expediente se evidencia que el reclamado ha vulnerado el artículo 5.1.d), *principio de exactitud*, en relación con el artículo 5 de la LOPGDD*, Exactitud de los datos*, al confundir en su identificación los datos de carácter personal del reclamante con los de un tercero con el mismo nombre y apellidos sin haber comprobado el DNI o pasaporte como marca el protocolo.

En relación con el citado artículo y su actualización (que sería la manifestación del principio de exactitud que podría entenderse incumplido), exige que se adopten *"las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan".*

Es decir, el artículo 5.1.d) no impone adoptar medidas desproporcionadas para actualizar los datos, sino las razonables, atendiendo a los medios disponibles y el fin para el que se usan los datos. Así lo expresa también el considerando 39 del RGPD.

Con relación a este principio, en el considerando 39 del RGPD entre otras cuestiones indica que *"(…) para garantizar que los datos personales no se conservan más tiempo del necesario, el responsable del tratamiento ha de establecer plazos para su supresión o revisión periódica. Deben tomarse todas las medidas razonables para garantizar que se rectifiquen o supriman los datos personales que sean inexactos".*

Considera el reclamante que una tercera persona ha utilizado su identidad para cambiar su adscripción a otro Centro de Salud y que interpuesta denuncia policial se ha dado nueva cita a la persona que usurpó su identidad, vulnerándose el principio de exactitud que debe regir en los datos de carácter personal, contemplado en el artículo 5.1.d) del RGPD, así como del artículo 5.1 de la LO 3/2018, de 5 de diciembre, de Protección de datos personales y garantía de los derechos digitales.

Principio de exactitud, 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 que *"Se averiguó que existe otro paciente que coincide en nombre y apellidos con el reclamante…De esta forma, una vez realizadas las averiguaciones pertinentes, se ha podido concluir que, sobre la ficha administrativa del reclamante se realizó un cambio en el domicilio del mismo al haberse atendido al ciudadano con el mismo nombre y apellidos, sin haber comprobado el DNI o pasaporte del solicitante".*

No obstante, en su escrito de 08/10/2021 señala que *"A su vez, debemos referenciar que en cumplimiento del principio de exactitud recogido en el artículo 5 del RGPD, según el cual, los datos tratados deben ser exactos y, si fuera necesario, actualizados; por parte del responsable del tratamiento, se han adoptado todas las*

medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos, y de forma proactiva, se ha procedido de oficio a cancelar de la historia clínica del reclamante los registros que no correspondían a su persona".

Y que por tanto *"queda constatado que, no se ha producido una suplantación de identidad del interesado, si no que el incidente ocurrido se debe a un error humano en la identificación de dos ciudadanos que tienen el mismo nombre y apellidos, habiéndose detectado el mismo, de manera proactiva, se han solventado las distintas consecuencias que pudieran haberse materializado".*

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

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

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

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

Por su parte, la LOPDGDD en su artículo 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".

(…)"

VI

El RGPD define las violaciones de seguridad de los datos personales como *"todas aquellas violaciones de la seguridad que ocasionen la destrucción, perdida o alteración accidental o ilícita de datos personales trasmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos".*

De la documentación obrante en el expediente se ofrecen indicios evidentes de que el reclamado ha vulnerado el artículo 32 del RGPD, al producirse un incidente de seguridad como consecuencia del quebrantamiento de las medidas establecidas para evitar errores en la identificación de los usuarios.

Hay que señalar que el RGPD en el citado precepto no establece un listado de las medidas de seguridad que sean de aplicación de acuerdo con los datos que son objeto de tratamiento, sino que establece que el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas que sean adecuadas al riesgo que conlleve el tratamiento, teniendo en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, alcance, contexto y finalidades del tratamiento, los riesgos de probabilidad y gravedad para los derechos y libertades de las personas interesadas.

Asimismo, las medidas de seguridad deben resultar adecuadas y proporcionadas al riesgo detectado, señalando que la determinación de las medidas técnicas y organizativas deberá realizarse teniendo en cuenta: la seudonimización y el cifrado, la capacidad para garantizar la confidencialidad, integridad, disponibilidad y resiliencia, la capacidad para restaurar la disponibilidad y acceso a datos tras un incidente, proceso de verificación (que no auditoría), evaluación y valoración de la eficacia de las medidas.

En todo caso, al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, como

consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos y que pudieran ocasionar daños y perjuicios físicos, materiales o inmateriales.

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

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

En el presente caso, tal y como consta en los hechos y en el marco del expediente de investigación E/10590/2020 la AEPD trasladó al reclamado el 08/10/2020 la reclamación presentada para que procediese a su análisis e informase a esta Agencia de las acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos.

El reclamado ha alegado en relación con lo indicado en el antecedente segundo de que no se había dado respuesta al traslado de la reclamación presentada, que todo ha sido debido a problemas en el registro de la oficina de internet, lo que provocó que no se pudiera tener acceso antes a las solicitudes enviadas por la Agencia Española de Protección de Datos, lo que ha supuesto que algunas notificaciones recibidas no se hayan podido atender en tiempo y forma.

No obstante, la responsabilidad del reclamado viene determinada por la quiebra de seguridad puesta de manifiesto por el 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 e impedir el acceso a los mismos en caso de incidente físico o técnico.

Parece evidente que en el presente caso no se siguieron las medidas establecidas para evitar errores en la identificación de los usuarios como se acredita en el informe emitido el 15/09/2021 por la Gerencia Asistencial de Atención Primaria en el que se describen los hechos ocurridos, indicando que: *"Al compartir nombre y apellidos, entendemos que se ha producido un problema de identificación univoca de ciudadanos al gestionar tanto las citas como el cambio den la base de datos poblacional de fecha 08/04/2020 debiendo reforzarse con los Centro de Salud implicados las actuaciones de seguridad en la tramitación de las citas para la identificación univoca de ciudadanos con el uso de lectores de banda magnética la citación mediante el DNI o pasaporte"* y que "*Tras el análisis realizado se concluyó que sobre la ficha administrativa del reclamante se realizó un cambio de domicilio desde el CS* ******CENTRO.1*** *cuando se atendió al ciudadano tipo "transeúnte," al coincidir sus datos de nombre y apellidos, sin haberse verificado los datos unívocos de DNI o pasaporte".*

Asimismo, el reclamado señalaba en su escrito de 08/10/2021: *"Así pues, se ha producido un problema en la identificación del ciudadano al haberse gestionado tanto las citas como el cambio en la base poblacional sin haberse aplicado las indicaciones previas respecto de identificación inequívoca..."*.

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

VII

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 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.

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".

En el presente caso, el reclamado ha vulnerado la normativa en materia de protección de datos de carácter personal tanto del principio de exactitud de los datos como del principio de seguridad de los mismos.

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

Hay que señalar que la LOPDGDD contempla en su artículo 77 la sanción de apercibimiento en relación con los tratamientos de datos personales que no se adecúen a sus previsiones. A este respecto, el artículo 83.7 del RGPD contempla que *"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, se contempla que la resolución que se dicte se podrán establecer medidas que proceda adoptar para que cese la conducta, se corrijan los efectos de la infracción que se hubiese cometido y su adecuación a las exigencias contempladas en los artículos 5.1.d) y 32 del RGPD, así como la aportación de medios acreditativos del cumplimiento de lo requerido.

No obstante, el reclamado ha reconocido el error cometido señalando que sobre la ficha administrativa del reclamante se realizó un cambio en el domicilio al haberse atendido a un ciudadano con el mismo nombre y apellidos sin haber comprobado el DNI o pasaporte, lo que provocó la vulneración del principio de exactitud y el quebrantamiento de las medidas de seguridad implantadas para la identificación de los usuarios en operaciones de cambio domicilio, así como para la

solicitud de citas, sistema aportado por el reclamado en el informe emitido el 15/09/2021 por la Gerencia Asistencial de Atención Primaria.

Por último, se indica que si bien las medidas señaladas para el personal que realiza estas funciones, ya se encontraban en conocimiento de los mismos, pues quincenalmente se actualiza el Espacio AP Madrid (espacio de información habitual para los profesionales de Atención Primaria), en la próxima actualización se incluirá nueva reseña en forma de *"Sabías que…",* incidiendo en la necesidad de la observación del protocolo establecido. También en los próximos cursos de formación se incidirá de forma expresa en el apartado de protección de datos e identificación de usuarios.

Por tanto, a la luz de lo que antecede, se considera que la respuesta del reclamado ha sido razonable, subsanando la incidencia no procediendo instar la adopción de medidas adicionales, al haber adoptado medidas de carácter técnico y organizativas de conformidad con la normativa en materia de protección de datos para evitar que se vuelvan a producirse situaciones como la que dio lugar a la presente reclamación, que es la finalidad principal de los procedimientos respecto de aquellas entidades relacionadas en el artículo 77 de la LOPDGDD.

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 a CONSEJERÍA DE SANIDAD de la COMUNIDAD DE MADRID. con CIF S7800001E, por una infracción de los artículos 32.1 y 5.1.d) del RGPD, tipificadas en los artículos 83.4.a) y 83.5.a) del RGPD, una sanción de apercibimiento.

SEGUNDO: NOTIFICAR la presente resolución a la CONSEJERÍA DE SANIDAD de la COMUNIDAD DE MADRID.

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