- **Procedimiento Nº: PS/00443/2019**

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, el reclamante) con fecha 5 de junio de 2019 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra ***SERVICIO ANDALUZ DE SALUD*** con NIF ***Q9150013B*** (en adelante, el reclamado). Los motivos en que basa la reclamación son en síntesis, que con fecha 16/04/2019 solicitó su historia clínica y le comunicaron que no se la pueden facilitar porque se ha perdido debido a que ha habido mudanzas; que solicitó el documento acreditativo de tal circunstancia hasta en dos ocasiones y finalmente se lo enviaron. Adjunta dicho documento.

SEGUNDO: Tras la recepción de la reclamación, la Subdirección General de Inspección de Datos procedió a realizar las siguientes actuaciones:

El 22/07/2019 fue trasladada al reclamado el escrito interpuesto para su análisis y comunicación a la denunciante de la decisión adoptada al respecto. Igualmente, se le requería para que en el plazo de un mes remitiera a la Agencia determinada información:

> - Copia de las comunicaciones, de la decisión adoptada que haya remitido al reclamante a propósito del traslado de esta reclamación, y acreditación de que el reclamante ha recibido la comunicación de esa decisión.
> - Informe sobre las causas que han motivado la incidencia que ha originado la reclamación.
> - Informe sobre las medidas adoptadas para evitar que se produzcan incidencias similares.
> - Cualquier otra que considere relevante.

El 02/08/2019 el reclamado dio respuesta al requerimiento de información señalando que la petición de documentación de historia clínica de la reclamante fue solicitada al Hospital Regional de ******LOCALIDAD.1***, a la Dirección Gerencia del mencionado centro hospitalario informe de los motivos que han causado la reclamación efectuada ante la AEPD, manifestando:

> 1.- Que han realizado una búsqueda exhaustiva de los documentos solicitados por la interesada, de la cual se ha obtenido respuesta negativa.
> 2.- Que no existen en las bases de datos ni en los archivos del Hospital Regional de ******LOCALIDAD.1***, registro alguno de actuaciones u/o atenciones realizadas a la reclamante antes del año 2007.
> 3.- Que toda la documentación generada a partir del 2007 le ha sido entregada a la reclamante.

TERCERO: El 26/11/2019, de conformidad con el artículo 65 de la LOPDGDD, la Directora de la Agencia Española de Protección de Datos acordó admitir a trámite la reclamación presentada por el reclamante contra el reclamado.

CUARTO: Con fecha 18/12/2019, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador al reclamado, por la presunta infracción del artículo 32 del RGPD, tipificada en el artículo 63.4.a) del citado Reglamento., considerando que la sanción que pudiera corresponder sería de APERCIBIMIENTO.

QUINTO: Notificado el acuerdo de inicio, el reclamado al tiempo de la presente resolución no ha presentado escrito de alegaciones, por lo que es de aplicación lo señalado en el artículo 64 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, que en su apartado f) establece que en caso de no efectuar alegaciones en el plazo previsto sobre el contenido del acuerdo de iniciación, éste podrá ser considerado propuesta de resolución cuando contenga un pronunciamiento preciso acerca de la responsabilidad imputada, por lo que se procede a dictar Resolución.

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

HECHOS PROBADOS

PRIMERO: El 05/06/2019 tiene entrada en la AEPD escrito del reclamante señalando que en fecha 16/04/2019 solicitó su historial clínico al Hospital Regional de ******LOCALIDAD.1*** y le comunicaron que no se la pueden facilitar porque se ha perdido debido a que ha habido mudanzas; solicitó el documento acreditativo de tal circunstancia hasta en dos ocasiones y finalmente se lo enviaron.

SEGUNDO: El Servicio Andaluz de Salud dependiente de la Consejería Salud y Familias en escrito de 05/03/2019 ha señalado que la reclamante solicito su historial clínico al Hospital Regional de ******LOCALIDAD.1*** con resultado negativo y solicitada información a la Gerencia del Hospital de los motivos ha informado que se había realizado una búsqueda exhaustiva de la documentación solicitada; que ni en la base de datos ni en los archivos del Hospital existen actuaciones realizadas a la reclamante con anterioridad a 2007 y que la documentación generada con posterioridad a dicha fecha le ha sido entregada a la reclamante.

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 el art. 47 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), la Directora de la Agencia Española de Protección de Datos es competente para resolver este procedimiento.

II

La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, en su artículo 64 *"Acuerdo de iniciación en los procedimientos de naturaleza sancionadora"*, dispone:

"1. El acuerdo de iniciación se comunicará al instructor del procedimiento, con traslado de cuantas actuaciones existan al respecto, y se notificará a los interesados, entendiendo en todo caso por tal al inculpado.

Asimismo, la incoación se comunicará al denunciante cuando las normas reguladoras del procedimiento así lo prevean.

2. El acuerdo de iniciación deberá contener al menos:

a) Identificación de la persona o personas presuntamente responsables.

b) Los hechos que motivan la incoación del procedimiento, su posible calificación y las sanciones que pudieran corresponder, sin perjuicio de lo que resulte de la instrucción.

c) Identificación del instructor y, en su caso, Secretario del procedimiento, con expresa indicación del régimen de recusación de los mismos.

d) Órgano competente para la resolución del procedimiento y norma que le atribuya tal competencia, indicando la posibilidad de que el presunto responsable pueda reconocer voluntariamente su responsabilidad, con los efectos previstos en el artículo 85.

e) Medidas de carácter provisional que se hayan acordado por el órgano competente para iniciar el procedimiento sancionador, sin perjuicio de las que se puedan adoptar durante el mismo de conformidad con el artículo 56.

f) Indicación del derecho a formular alegaciones y a la audiencia en el procedimiento y de los plazos para su ejercicio, así como indicación de que, en caso de no efectuar alegaciones en el plazo previsto sobre el contenido del acuerdo de iniciación, éste podrá ser considerado propuesta de resolución cuando contenga un pronunciamiento preciso acerca de la responsabilidad imputada.

3. Excepcionalmente, cuando en el momento de dictar el acuerdo de iniciación no existan elementos suficientes para la calificación inicial de los hechos que motivan la incoación del procedimiento, la citada calificación podrá realizarse en una fase posterior mediante la elaboración de un Pliego de cargos, que deberá ser notificado a los interesados".

En aplicación del anterior precepto y teniendo en cuenta que no se han formulado alegaciones al acuerdo de inicio, procede resolver el procedimiento iniciado.

III

El artículo 58 del RGPD, *Poderes*, señala:

"2. Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:

(…)

b) sancionar a todo responsable o encargado del tratamiento con apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento;
i) imponer una multa administrativa con arreglo al artículo 83, además o en lugar de las medidas mencionadas en el presente apartado, según las circunstancias de cada caso particular;
(…)"

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".

IV

La Ley 41/2002, de 14 de noviembre, reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, en su artículo 17, dedicado por completo a la conservación de la documentación clínica, establece en su punto primero que *"Los centros sanitarios tienen la obligación de conservar la documentación clínica en condiciones que garanticen su correcto*

mantenimiento y seguridad, aunque no necesariamente en el soporte original, para la debida asistencia al paciente durante el tiempo adecuado a cada caso y, como mínimo, cinco años contados desde la fecha del alta de cada proceso asistencial" y en su apartado 6 determina lo siguiente: *"Son de aplicación a la documentación clínica las medidas técnicas de seguridad establecidas por la legislación reguladora de la conservación de los ficheros que contienen datos de carácter personal y, en general, por la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal".*

El artículo 19 de la citada Ley 41/2002 indica: *"Derechos relacionados con la custodia de la historia clínica. El paciente tiene derecho a que los centros sanitarios establezcan un mecanismo de custodia activa y diligente de las historias clínicas. Dicha custodia permitirá la recogida, la integración, la recuperación y la comunicación de la información sometida al principio de confidencialidad con arreglo a lo establecido por el artículo 16 de la presente Ley".*

Los hechos puestos de manifiesto en la presente reclamación se concretan en la existencia de una brecha de seguridad en los sistemas de la reclamada permitiendo la vulnerabilidad del mismo al acreditarse que la historia clínica de la reclamante con anterioridad al año 2007 no les consta en la base de datos ni en los archivos del Hospital General de Málaga.

En el RGPD se definen las violaciones a la 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 evidencia que el reclamado ha vulnerado el artículo 32.1 del RGPD, al producirse una violación de la seguridad de sus sistemas al permitirse la perdida de documentación clínica relativa a la reclamante. El propio reclamado en escrito de 02/08/2019 ha señalado que la petición de documentación relativa a la historia clínica de la reclamante fue solicitada al Hospital Regional de Málaga, y la Gerencia del mencionado centro hospitalario informó de los motivos de la reclamación manifestando que se había realizado una búsqueda exhaustiva de los documentos solicitados por la interesada y que el resultado había sido negativo y que no existen en las bases de datos ni en los archivos del Hospital Regional de Málaga, registro alguno de actuaciones o atenciones realizadas a la reclamante antes del año 2007.

Hay que señalar, que en la actualidad el RGPD 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 deberán aplicar las 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.

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".

V

La vulneración del artículo 32.1 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 otra parte, la LOPDGDD en su artículo 71, *Infracciones*, señala que:

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

Y 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 evidencian la vulnerabilidad de las medidas de seguridad implantadas por el reclamado provocando la pérdida del historial clínico de la reclamante, lo que constituye una infracción del artículo 32.1 del RGPD.

VI

No obstante, 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".

De conformidad con las evidencias de las que se dispone y sin perjuicio de lo que resulte de la instrucción del procedimiento, dicha conducta podría constituir en principio por parte del reclamado la posible infracción a lo dispuesto en el artículo 32 del RGPD.

No obstante, 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 caso examinado ha quedado acreditado que el reclamado no tiene adoptadas medidas técnicas y organizativas que garanticen un nivel de seguridad adecuado capaz de asegurar la confidencialidad, integridad y disponibilidad de los datos evitando su perdida.

Se hace necesario señalar que no corregir dichas circunstancias adoptando las medidas técnicas y organizativas adecuadas de conformidad con lo señalado en el artículo 32.1 del RGPD o bien reiterar la conducta puesta de manifiesto en la reclamación y que es causa del presente procedimiento, así como no informar seguidamente a esta AEPD de las medidas adoptadas podría dar lugar al ejercicio de posibles actuaciones ante el responsable del tratamiento a fin de que se apliquen de manera efectiva las medidas apropiadas para garantizar y no comprometer la confidencialidad de los datos de carácter personal y el derecho a la intimidad de las personas.

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 SERVICIO ANDALUZ DE SALUD, con NIF ***Q9150013B***, por una infracción del aartículo 32.1 del RGPD, tipificada en el artículo 83.4.a) del RGPD, una sanción de apercibimiento.

SEGUNDO: REQUERIR a SERVICIO ANDALUZ DE SALUD, con NIF **Q9150013B,** para que en el plazo de un mes desde la notificación de esta resolución, acredite: la adopción de las medidas de seguridad necesarias y pertinentes de conformidad con la normativa en materia de protección de datos de carácter personal a fin de evitar que en el futuro vuelvan a producirse incidencias como las que han dado lugar a la reclamación corrigiendo los efectos de la infracción producida, adecuando las citadas medidas a las exigencias contempladas en el artículo 32.1 del RGPD.

SEGUNDO: NOTIFICAR la presente resolución a ***SERVICIO ANDALUZ DE SALUD,*** con NIF ***Q9150013B***.

TERCERO: 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.

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