- **Procedimiento Nº: PS/00250/2021**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: Las actuaciones de inspección se inician por la recepción de un escrito de reclamación de ***A.A.A.*** (en adelante, el reclamante), en el que manifiesta que se han producido accesos indebidos a su historia clínica por parte de una trabajadora del Servicio Extremeño de Salud (en adelante SES), con categoría profesional de enfermera. Los accesos se realizan sin la autorización del reclamante y sin que medie una relación que lo justifique.

El reclamante añade que los accesos indebidos están perfectamente identificados en el Certificado de accesos al historial clínico, emitido el 14/08/2020 por la Gerencia del Área de Salud de Badajoz del Servicio Extremeño de Salud (SES) en contestación del oficio librado por el Juzgado de Instrucción nº 2 de Badajoz, en el que constan 5 accesos producidos entre el 02/10/2007 al 15/07/2019. Indica que faltan más accesos indebidos, que están pendientes de obtención por el Juzgado.

Documentación relevante aportada por el reclamante:

-Autos emitidos por el Juzgado de instrucción nº 2 de Badajoz admitiendo a trámite querella por revelación de secretos y acordando práctica de pruebas.

-Certificado de accesos al historial clínico obrante en el sistema de información del SES del reclamante de fecha 14/08/2020.

SEGUNDO: A la vista de los hechos notificados y de los documentos aportados por el SES, la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos descritos en los apartados anteriores, 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), teniendo conocimiento de los siguientes extremos:

ANTECEDENTES

Fecha en la que tuvieron lugar los hechos reclamados: 15 de julio de 2019

Fecha de entrada de la reclamación: 13 de octubre de 2020

Reclamante: ***A.A.A.*** (el reclamante)

Reclamado: SERVICIO EXTREMEÑO DE SALUD (SES)
ENTIDADES INVESTIGADAS

SERVICIO EXTREMEÑO DE SALUD, con NIF S0611001I, y con domicilio en Avda. de las Américas 2, 06800 Mérida, Badajoz.

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

Con fecha 12/11/2020 se trasladó la reclamación al SES en el marco de las actuaciones de referencia E/9118/2020. El documento de traslado fue recogido el día 23/11/2020 según su acuse de recibo. Pasado el plazo concedido, el día 10/02/2021 se dicta resolución admitiendo la reclamación e instando las presentes actuaciones de inspección.

Con fecha 16/02/2021 se requirió información y documentación sobre los hechos al SES, no habiendo recibido respuesta a la fecha de realización del presente informe. El requerimiento fue recogido el día 22/02/2021, según acuse de recibo. Se adjunta al requerimiento efectuado el documento de traslado de la reclamación emitido anteriormente, indicando que no consta contestación al mismo.

En el requerimiento realizado se solicitaba la siguiente información al SES:

1.- Copia del informe elaborado y documentación acreditativa en relación con los hechos, que contendrá los siguientes aspectos:

> 1–1. Especificación detallada de las causas que han hecho posible los hechos.
>
> 1–2. Descripción detallada de las acciones tomadas con objeto de minimizar los efectos adversos y para la resolución final del incidente, indicando fecha y hora de las medidas adoptadas.
>
> 1-3. Medidas adoptadas para evitar que se produzcan incidencias similares, fechas de implantación y controles efectuados para comprobar su eficacia.

2.- Respecto de la seguridad de los tratamientos de datos personales con anterioridad a los hechos:

> 2-1. Documentación acreditativa del Análisis de Riesgo que ha conllevado la implantación de las medidas de seguridad y copia de las Evaluaciones de Impacto, en su caso.
>
> 2-2. Detallar aquellas medidas técnicas y organizativas adoptadas para garantizar un nivel de seguridad adecuado a los riesgos detectados con relación a los accesos por el personal sanitario a los historiales clínicos de los pacientes. Política de seguridad adoptada por la entidad con relación a ello.

No obstante, con fecha 05/04/2021 se recibe contestación del SES al traslado realizado el 12/11/2020 en el marco de las actuaciones de referencia E/09118/2020, en los siguientes términos:

“I. SOBRE LOS ANTECEDENTES

Solicita el citado escrito a esta Administración Pública que se pronuncie respecto de una reclamación recibida por parte del ciudadano -el reclamante- en fecha 13 de octubre de 2020.

En dicha comunicación se solicita:

- *La decisión adoptada a propósito de esta reclamación.*
- *En el supuesto de ejercicio de los derechos regulados en los artículos 15 a 22 del RGPD, acreditación de la respuesta facilitada al reclamante.*
- *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, fechas de implantación y controles efectuados para comprobar su eficacia.*
- *Cualquier otra que considere relevante.*
- *En este sentido, el presente documento da cumplimiento a dicha solicitud, aportando en el Anexo 1 las comunicaciones con el reclamante y, en el resto de apartados de este documento, la información solicitada por la AEPD.*

II. SOBRE LOS CONTROLES DE ACCESO YA ESTABLECIDOS EN EL SERVICIO EXTREMEÑO DE SALUD

El Servicio Extremeño de Salud (en adelante, SES) es un organismo autónomo de carácter administrativo, dependiente de la Consejería de Sanidad y Dependencia de la Junta de Extremadura que tiene encomendado ejercer las competencias de administración y gestión de servicios, prestaciones y programas sanitarios que rige su funcionamiento por las normativas nacional y autonómica que le son de aplicación.

En este sentido, la Ley de la Comunidad Autónoma de Extremadura 3/2005, de 8 de julio, de información sanitaria y autonomía del paciente regula en su artículo 35.3 el derecho del paciente tanto de acceso y obtención de copias o certificados de los documentos que obran en su historia clínica, como de “conocer en todo caso quién ha accedido a sus datos sanitarios, el motivo del acceso y el uso que se ha hecho de ellos”. Pues bien, sobre el ejercicio de este derecho, que se ha solicitado por parte del reclamante, no se puede colegir de la documentación aportada que haya existido incumplimiento alguno por parte de esta Administración pues, a la vista está que esta información obra en manos del denunciante.

Traducido este derecho al sistema de información que soporta la información clínica de los pacientes en el Servicio Extremeño de Salud, debe apuntarse que la ejecución efectiva de este derecho a conocer quién y para qué se accede a la Historia Clínica, se traduce en la necesaria existencia de una relación que legitime el acceso del profesional sanitario a una determinada Historia Clínica. Por este motivo, al acceder al Historial de un paciente que se está tratando en ese momento en el puesto de trabajo clínico (sea Hospitalización, Consultas Externas, Pruebas Funcionales, Hospital de Día, Quirófano…), el sistema informático entiende de forma automática que el motivo de acceso es Asistencial, y así se refleja en dicho sistema. No obstante, este no es un

proceso automático, sino que el sistema sólo permite el acceso a historiales de pacientes que, bien están bajo un tratamiento activo, bien están citados en la agenda del profesional o, bien pertenecen a los pacientes que tiene asignados en su cupo.

Cuando se accede al Historial médico mediante la búsqueda de un paciente (no seleccionándolo directamente de un listado de trabajo), el sistema obliga a elegir un motivo de acceso de entre los que están configurados para cada perfil. En este sentido, a un facultativo de Atención Especializada le aparecerán los siguientes:

- *El motivo Gestión de Paciente se selecciona cuando el acceso al Historial se relaciona con una acción que se va a realizar sobre un paciente que no se encuentra en el Puesto de Trabajo Clínico en ese momento, tal como consulta o revisión de documentación, realización de informes, preparación previa de consulta o intervención quirúrgica, revisión de órdenes clínicas y citaciones…*

- *El motivo Estudio de Investigación se selecciona, como su propio nombre indica, cuando el acceso al Historial médico se relaciona con trabajos de investigación en los que está incluido ese paciente.*

- *El motivo Solicitud DCL se usará cuando el acceso al Historial se realice para dar respuesta a una Solicitud de Documentación Clínica procedente del propio paciente o de alguna persona autorizada.*

- *El motivo Incapacidad Laboral sólo lo tienen disponible perfiles de Inspección y lo seleccionarán cuando el acceso al Historial esté relacionado con un problema laboral del paciente.*

- *El Acceso SOLO a la Agenda del Paciente no es un motivo de acceso al Historial; es la denominación con la que queda identificado el acceso a la Agenda en el log de registros de accesos a la Agenda del paciente.*

No obstante, aunque se haya establecido este filtro de acceso, ello no implica que el acceso sea total, puesto que cada uno de los motivos que legitimaría el acceso y que acaban de exponerse no implica el acceso sin restricciones a la información clínica. Por ello, cada uno de los accesos va acompañado de restricciones de acceso, puesto que no tendría sentido un acceso total a información sanitaria cuando el motivo que justifica el acceso es un motivo administrativo.

De esta manera, la normativa sanitaria pública extremeña por la que se rige el SES, es una normativa que ofrece mayores derechos a los ciudadanos respecto de su información clínica; ello con el reconocimiento del derecho a conocer quién ha accedido a su información sanitaria. El ejercicio de este derecho, así como la garantía de la confidencialidad de la información sanitaria tratada en el SES se hace efectiva mediante los controles de acceso a la información clínica.

Cabe colegir por tanto que, los accesos a que se refiere el denunciante se dieron cumpliéndose los requisitos de legitimidad de acceso que de desprenden de las obligaciones de la normativa de protección de datos y de las propias impuestas de manera interna desde el Servicio Extremeño de Salud. Así, en el Hecho SEGUNDO que se usa como argumento, debe desecharse la idea de que, como se apunta, el

acceso se hizo prevaliéndose de su "categoría profesional de enfermera", puesto que, de no darse las situaciones descritas en este apartado, el acceso no hubiera sido posible. Por tanto, no cabe entender como válido el argumento utilizado de que se produjo un acceso "sin que mediara entre ellos una relación asistencial de enfermero/paciente" dado que el sistema solicita para el acceso a información clínica la existencia de un motivo que legitime el acceso.

Asimismo, deben desecharse también los argumentos descritos en el Hecho TERCERO, donde se apuntan los accesos realizados por la ***Señora B.B.B.****, ya que todos los accesos a la información debieron y, así lo fueron, motivados por alguno de los escenarios previstos y detallados con anterioridad.*

III. SOBRE EL FORO

No procura esta parte poner en cuestión la autoridad de la AEPD, ni las informaciones aportadas por el denunciante; no obstante, el SES en su responsabilidad no estima oportuno atender denuncias o solicitudes que no partan de una base sólida. En este sentido, el Hecho PRIMERO del escrito presentado por el denunciante hace referencia a hechos que, bien deben entenderse como subjetivos o, al menos, difícilmente objetivables, tales como el ejercicio de "un estricto control sobre la vida y la persona" que no permitió al denunciante "desarrollar una vida normal y rehacer su vida sentimental".

Al no tratarse de información objetivable, el SES estima que no debe pronunciarse en este sentido y que, más bien, corresponde a otro ámbito, concretamente a los órganos judiciales, establecer si los hechos son como se denuncian. Entiéndase, entonces, que existe un ánimo de esta Administración de colaborar, en tanto en cuanto le sea posible, pero que se entiende que los hechos denunciados bien tienen que ver con acciones u omisiones tipificadas en el Código Penal sobre las que el SES no pude hacer otra cosa más que colaborar con los órganos judiciales que las diriman.

Definida la legitimidad de los accesos a la información de un paciente (el denunciante) por parte de una trabajadora del sistema sanitario público (la denunciada), dado que sin la existencia de dicha legitimidad el acceso sería técnicamente imposible, el SES entiende que la situación denunciada debe esperarse a que tenga la condición de Hecho Probado (entendido éste como el relato de sucesos objeto de enjuiciamiento que el órgano judicial ha considerado ciertos). Ello, porque además se entiende que los hechos denunciados no se corresponden con un incumplimiento de la normativa de protección de datos del SES como Responsable del Tratamiento si no, más bien como un delito (que bien podría tipificarse de revelación de secretos) cometido por una persona, eso sí, trabajadora del SES, en un ámbito privado en el que el SES como empleador no tiene alcance.

Si, mediando una sentencia que establezca los hechos denunciados como hechos probados, teniendo el SES conocimiento de los mismos, se emprenderán las medidas internas oportunas basándonos en el Régimen interno tal como se describe en los avisos legales de los inicios de sesión de los usuarios del sistema de información. Hasta ese momento, entiende el SES que debe archivarse el presente procedimiento y, caso de producirse sentencia favorable al denunciado comunicárselo al SES para que se establezcan las sanciones internas que correspondan.

IV. SOBRE EL CUMPLIMIENTO DE LAS OBLIGACIONES DEL SES COMO RESPONSABLE DEL TRATAMIENTO

Por otra parte, respecto de las obligaciones del Servicio Extremeño de Salud, como responsable del tratamiento, y coordinadamente con lo expuesto en el inicio de la alegación Segunda (II), el SES ha venido cumpliendo sus obligaciones como responsable del Tratamiento respecto de las solicitudes hechas por el denunciante. Se apuntaba en la citada alegación la existencia, fruto del desarrollo legislativo extremeño de un derecho a "conocer quien accede a la información clínica" y, vista la información aportada por el denunciante, cabe entender que el SES ha cumplido dichas obligaciones.

Cuestión distinta es, si el denunciante entiende que la persona denunciada ha incumplido sus obligaciones de confidencialidad y, de ser así, una vez se muestre como hecho probado, podrá dirigirse al SES para que se tomen las medidas oportunas.

V. SOBRE LAS MEDIDAS YA APLICADAS POR EL SES

Previo a tener conocimiento de la denuncia que se traslada, el SES, en el ámbito de su responsabilidad proactiva ya había tomado medidas que garantizan la confidencialidad de la información.

(1) Control de acceso: el acceso a la información clínica de los pacientes en el Servicio Extremeño de Salud solo se da cuando se cumplen las normas de control de acceso;

a. En primer lugar, el control de acceso a la información está segregada en función del rol profesional del sistema de información, esto es, sólo acceden aquellos que, por motivo de sus funciones y obligaciones deban a acceder a información clínica y, dentro de éstos, en función de la finalidad se tiene acceso a todo o a parte de dicha información.

b. Estando legitimado al acceso a la información clínica por el rol profesional, el acceso a los datos de los ciudadanos no es libre para los usuarios, debiendo mediar una relación que legitime el acceso a los datos concretos, a saber, formar parte del "cupo" del profesional sanitario, tenerlo citado en la agenda o que se encuentre en un tratamiento activo. De no darse esas circunstancias, el acceso no es posible.

c. Concedido, en su caso, el acceso habiéndose dado las dos circunstancias anteriores, éste no necesariamente es un acceso total o un acceso a la Historia Clínica completa ya que los accesos están definidos para finalidades concretas y éstas, a su vez, han definido a qué información dan acceso en base a dicha finalidad.

Hablamos, por tanto, de una doble legitimación basada en (1) el rol profesional y (2) la finalidad del acceso y, ello sumado a la necesidad de la existencia de un motivo que legitime el acceso.

(2) Aviso legal al inicio de la sesión en el que se recuerda a los usuarios que la información a la que se accede es confidencial y que sólo debe ser tratada con la finalidad que legitima el acceso.
Los usos ajenos a los fines anteriores son considerados inapropiados y podrían considerarse falta laboral o, en su caso, delito y dar lugar a la incoación de expediente en el ámbito legal correspondiente.

"[…]Es contrario a la buena fe el intento de acceso a información para la que no se tiene permisos ni privilegios o que no esté directamente relacionada con sus funciones, así como filtración de cualquier tipo de dato, especialmente de carácter personal, fuera de la red corporativa.

En este sentido, el usuario del sistema informático […] conoce las responsabilidades establecidas en el Código Penal, en la normativa de Protección de Datos y en el resto de la legislación española sobre el uso ilícito, contrario a la moral, a la buena fe y las costumbres de las herramientas informáticas, sin perjuicio de la responsabilidad derivada de la normativa interna aplicable.

Al objeto de garantizar el cumplimiento de la política de seguridad, el SES podrá supervisar las comunicaciones y/o archivos recibidos/enviados por los usuarios por medio de los recursos y sistemas de la entidad en el caso de que existan sospechas fundadas de que se está haciendo un uso indebido de los recursos. […]"

La aceptación de este aviso legal es preceptiva para poder acceder al sistema de información.

(3) Píldoras formativas, recordatorios, circulares… respecto de los deberes de secreto y confidencialidad, consejos de seguridad y similares que, desde la Subdirección de Sistemas de Información junto con la figura del Delegado de Protección de Datos se lanzan a todos los usuarios del sistema, así como otros recursos accesibles desde el "portal del SES" a la que tienen acceso todos los usuarios del sistema de información del SES.

TERCERO: Con fecha 26 de mayo de 2021, 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, Artículo 5.1.f) del RGPD, tipificada en el Artículo 83.5 del RGPD.

CUARTO: Notificado el acuerdo de inicio del presente procedimiento sancionador, el SES, en calidad de responsable, no ha presentado alegaciones.

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: Consta acreditado que un tercero ajeno al reclamante accedió indebidamente a su historial clínico obrante en el SES, en diversas ocasiones sin que el SES interviniera para evitarlo una vez conocido el incidente.

SEGUNDO: La causa que ocasionó el acceso indebido fue la falta de medidas técnicas y organizativas implantadas en el sistema de información y control de accesos del SES.

TERCERO: Consta que un tercero ajeno tuvo conocimiento de los datos del reclamante obrantes en el historial clínico del SES categorizados como especiales según señala el art. 9 del RGPD.

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

Establece el artículo 5.1.f) del RGPD lo siguiente:

"Artículo 5 Principios relativos al tratamiento

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 acreditado que los datos personales del reclamante relativos a su historial médico que figuran en el sistema de información del SES fueron indebidamente accedidos por tercera persona ajena, vulnerando los principios de integridad y confidencialidad, ambos establecidos en el citado artículo 5.1.f) del RGPD.

III

Establece el artículo 32 del RGPD, *seguridad del tratamiento*, lo siguiente:

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 (El subrayado es de la AEPD).

El considerando 75 del RGPD enumera una serie de factores o supuestos asociados a riesgos para las garantías de los derechos y libertades de los interesados:

"Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados."

En el presente caso, de las actuaciones de investigación llevadas a cabo la selección del motivo de acceso a la historia clínica de un paciente del SAS no se verifica con el perfil de acceso del usuario quedando, en consecuencia, el acceso a la información a la discrecionalidad del usuario que accede.

Por lo tanto, como consecuencia de la falta de implantación de medidas técnicas y organizativas adecuadas de obligado cumplimiento por las Administraciones Públicas conforme señala el RD 3/2010, por el que se regula el Esquema Nacional de Seguridad (ENS), ha provocado el acceso por tercera persona ajena a los datos alojados en el sistema de información de historiales clínicos del SES. No consta la realización del preceptivo análisis de riesgos y, en su caso, evaluación de impacto acto sobre el tratamiento de datos de salud de los pacientes del SAS. Tampoco consta que el SAS tenga implantado un proceso de verificación, evaluación y valoración continua

de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

IV

De las actuaciones practicadas consta la ausencia de medidas de seguridad adecuadas tanto de índole técnica como organizativas, con las que contaba el SES realiza operaciones de tratamiento en relación con los datos de salud de los historiales clínicos. Tampoco consta la adecuación de las operaciones de tratamiento del SES al Esquema Nacional de Seguridad en el momento de producirse los accesos indebidos.

La consecuencia de esta implantación de medidas deficientes de seguridad fue la exposición a tercera persona ajena de los datos personales relativos a la salud del reclamante. Es decir, el afectado se ha visto desprovisto del control sobre sus datos personales relativos a su historial clínico.

Hay que añadir que, en relación con la categoría de datos a la que tercera persona ajena ha tenido acceso, se encuentran en la categoría de especiales según lo dispuesto en el art. 9 del RGPD, circunstancia que supone un riesgo añadido que se ha de valorar en el estudio de gestión de riesgos y que aumenta la exigencia del grado de protección en relación con la seguridad y salvaguarda de la integridad y confidencialidad de estos datos.

Este riesgo debe ser tenido en cuenta por el responsable del tratamiento quien debe establecer las medidas técnicas y organizativas necesarias que impida la pérdida de control de los datos por el responsable del tratamiento y, por tanto, por parte de los titulares de los datos que se los proporcionaron.

V

El artículo 83.4.a) del RGPD, señala lo siguiente:
(…)

“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”.

El artículo 83.5.a) del RGPD, señala lo siguiente:
(…)

“5. 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";

El artículo 76 de la LOPDGDD bajo la rúbrica "*Sanciones y medidas correctivas* ", señala lo siguiente:

> *1. Las sanciones previstas en los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679 se aplicarán teniendo en cuenta los criterios de graduación establecidos en el apartado 2 del citado artículo.*
>
> *1. Será posible, complementaria o alternativamente, la adopción, cuando proceda, de las restantes medidas correctivas a las que se refiere el artículo 83.2 del Reglamento (UE) 2016/679.*

VI

Establece el artículo 71 de la LOPDGDD, bajo la rúbrica "*Infracciones*" lo siguiente: *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.*

Establece el artículo 72.1.a) de la LOPDGDD, bajo la rúbrica "*Infracciones consideradas muy graves*", lo siguiente:

"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."

En el presente caso concurren las circunstancias infractoras previstas en el artículo 72.1.a) de la LOPDGDD arriba transcrito.

Establece el artículo 73 de la LOPDGDD, bajo la rúbrica "*Infracciones consideradas graves*" lo siguiente:

"*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.

En el presente caso concurren las circunstancias infractoras previstas en el artículo 73 apartado f) de la LOPDGDD arriba transcrito.

VII

Establece la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en el Capítulo III relativo a los "*Principios de la Potestad sancionadora*", en el artículo 28 la bajo la rúbrica "*Responsabilidad*", lo siguiente:

"1. Sólo podrán ser sancionadas por hechos constitutivos de infracción administrativa las personas físicas y jurídicas, así como, cuando una Ley les reconozca capacidad de obrar, los grupos de afectados, las uniones y entidades sin personalidad jurídica y los patrimonios independientes o autónomos, que resulten responsables de los mismos a título de dolo o culpa"

La falta de diligencia a la hora de implementar las medidas apropiadas de seguridad con la consecuencia del quebranto del principio de confidencialidad, constituye el elemento de la culpabilidad.

VIII

El artículo 58.2 del RGPD, señala lo siguiente*:*

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

b) dirigir a todo responsable o encargado del tratamiento un apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento;

Por su parte, el ordenamiento jurídico español ha optado por no sancionar con la imposición de multa administrativa a las entidades públicas, como es el SES, tal como se indica en el artículo 77.1. c) y apartados 2, 4, 5 y 6 de la LOPDDGG:

<<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.

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.

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.>>

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 EXTREMEÑO DE SALUD***, con NIF ***S0611001I***, por la infracción del Artículo 32 del RGPD tipificada en el Artículo 83.4.a) del RGPD la sanción de APERCIBIMIENTO, y por la infracción de artículo 5.1.f) del RGPD, tipificada en el Artículo 83.5.a) del RGPD, la sanción de APERCIBIMIENTO.

SEGUNDO: NOTIFICAR la presente resolución a ***SERVICIO EXTREMEÑO DE SALUD***.

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.

938-131120

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