- **Expediente N.º: EXP202201746**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: En fecha 27 de enero de 2022, tuvo entrada en la Agencia Española de Protección de Datos (en adelante, AEPD) escrito de reclamación, presentado por ***A.A.A.*** (en adelante, la parte reclamante)

La reclamación se dirige contra *SERVICIO CANARIO DE LA SALUD* con NIF *Q8555011I* (en adelante, la parte reclamada).

Los motivos en que basa la reclamación son los siguientes:

La reclamante manifiesta que se han producido accesos indebidos a su historia clínica y se ha revelado a terceros el diagnóstico.

Asimismo manifiesta que la web de la Consejería de Sanidad del Gobierno de Canarias (https://www.gobiernodecanarias.org/sanidad/) utiliza cookies sin tener aviso de las mismas ni disponer de una política de cookies y sin solicitar el consentimiento expreso para su utilización. Tampoco disponen de una Política de Privacidad.

Fecha en la que tuvieron lugar los hechos reclamados: 2 de noviembre de 2021.

Documentación relevante aportada por la parte reclamante:

- Respuesta emitida por el SERVICIO CANARIO DE LA SALUD respecto a accesos a la Historia Clínica, donde figuran Listado de Accesos realizados por Atención Primaria desde el 5/10/21 hasta el 9/12/2021 y Listado de Accesos realizados por Atención Especializada en Hospital General de Fuerteventura desde el 6/10/2021 al 10/12/2021.

En este documento la reclamante manifiesta que los accesos marcados en color no se asocian a ningún proceso clínico o consulta.

SEGUNDO: De acuerdo con el mecanismo previo a la admisión a trámite de las reclamaciones que se formulan ante la AEPD, previsto en 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 lo sucesivo, LOPDGDD), que consiste en dar traslado de las mismas a los delegados de protección de datos designados por los responsables o encargados del tratamiento, o a éstos cuando no los hubieren designado, y con la finalidad señalada en el referido artículo, se dio traslado de la reclamación a SERVICIO CANARIO DE LA SALUD (en adelante, la parte reclamada) para que procediera a su análisis y diera respuesta en el plazo de un mes, lo que se ha verificado mediante escrito de fecha de entrada en esta Agencia de 6 de mayo de 2022.

En respuesta al traslado y solicitud de información, la parte reclamada manifestó que había trasladado la reclamación a la Oficina de Seguridad (ODS) del Área de Servicios

Electromédicos y de la Información (ASEI) y a la Gerencia de Servicios Sanitarios de Fuerteventura.

El ASEI manifiesta haber procedido a auditar los accesos marcados por la reclamante solicitando a las personas que accedieron la justificación de tales accesos. La Gerencia de Servicios Sanitarios de Fuerteventura manifestó que, revisados los archivos obrantes en este centro directivo, no constaba “documentación que guarde relación con el expediente de referencia”.

Con fecha 25 de abril, la Secretaría General de la parte reclamada remitió el resultado de la auditoría realizada por el ASEI y manifestó a la AEPD que se remitió escrito a todas las gerencias en los siguientes términos:

"*La Agencia Española de Protección de Datos ha remitido, en un corto espacio de tiempo, varias reclamaciones relativas a accesos supuestamente indebidos a la historia clínica de pacientes por parte de personal del centro.*

La Instrucción n.º 4/10 de esta Dirección, relativa a la actuación del personal del Servicio Canario de la Salud que, con motivo del desempeño de su puesto de trabajo, trata datos de carácter personal, deja claro que en los órganos prestadores de servicios, el responsable del centro asistencial determinará qué unidades adoptarán, en nombre del responsable del tratamiento, las medidas necesarias para que el personal de cada unidad conozca, de forma comprensible, las normas de seguridad de los ficheros que afecten al desarrollo de sus funciones (apartado quinto).

En este sentido, es importante que el personal que accede a la historia clínica conozca las responsabilidades disciplinarias e incluso penales en las que puede incurrir si, pese a la advertencia que ya aparece en la aplicación, accede a la historia clínica de un paciente por motivos no justificados.

Del mismo modo se les recuerda que, ante cualquier indicio de accesos indebidos, la gerencia correspondiente deberá adoptar las medidas necesarias para depurar las responsabilidades administrativas o penales a que hubiere lugar".

La parte reclamada asimismo añadió que se había considerado conveniente elaborar un protocolo para la tramitación de las solicitudes recibidas en las que la persona interesada solicite información sobre quién accedió a su historia clínica.

TERCERO: En fecha 17 de mayo de 2022 tras analizarse la documentación que obraba en el expediente, se dictó resolución por la Directora de la Agencia Española de Protección de Datos, acordando el archivo de la reclamación.

La resolución fue notificada a la parte recurrente en fecha 17 de mayo, a través del Servicio de Notificaciones Electrónicas y Dirección Electrónica Habilitada según certificado que figura en el expediente.

CUARTO: En fecha 13 de junio de 2022, la parte reclamante interpuso un recurso potestativo de reposición contra dicha resolución, en el que alegaba que ha habido accesos no autorizados a su historia clínica y revelación de sus datos de salud a personal del hospital sobre los que no se ha resuelto, señalando que el Servicio

Canario de Salud se limita a indicar que "*ha auditado los acceso marcados por la parte reclamante"*, sin justificar cada uno de esos accesos y los motivos que llevó al personal en cuestión a acceder, ya que dichos accesos y movimientos en su historial clínico no se asocian a ningún proceso clínico ni visita médica.

QUINTO: En fecha 27 de julio de 2022 se remitió el recurso interpuesto a la parte reclamada en el marco de lo establecido en el artículo 118.1 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP) a los efectos de que formulase las alegaciones y presentase los documentos y justificantes que estimase procedentes.

La remisión del traslado fue notificada en fecha 27 de julio de 2022, a través del Servicio de Notificaciones Electrónicas y Dirección Electrónica Habilitada según certificado que figura en el expediente, no habiéndose aportado alegaciones por la parte reclamada a lo manifestado por la parte recurrente en el recurso de reposición presentado.

Dicho trámite fue notificado en fecha 27 de julio de 2022, no habiéndose recibido ninguna alegación de la parte reclamada a fecha de la actual resolución.

SEXTO: Con fecha 6 de octubre de 2022, se estima el recurso de reposición interpuesto por ***A.A.A.*** contra la resolución de esta Agencia dictada en fecha 17 de mayo de 2022, por la que se acordaba el archivo de la reclamación referida a SERVICIO CANARIO DE LA SALUD.

SEPTIMO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de las funciones asignadas a las autoridades de control en el artículo 57.1 y de los poderes otorgados en el artículo 58.1 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 LOPDGDD, teniendo conocimiento de los siguientes extremos:

El *SERVICIO CANARIO DE SALUD* está encuadrado dentro de la *CONSEJERÍA DE SANIDAD DEL GOBIERNO DE CANARIAS*.

En fecha 5 de diciembre de 2022, desde la Inspección de Datos se accede a la web de la *CONSEJERÍA DE SANIDAD DEL GOBIERNO DE CANARIAS* https://www.gobiernodecanarias.org/sanidad/ verificando que no dispone de un apartado sobre Política de Privacidad. No hay constancia de que se recaben datos en esta web.

En la web consta un aviso sobre cookies "*Este portal web utiliza cookies propias y de terceros para recopilar información que ayuda a optimizar su visita. Las cookies no se utilizan para recoger información de carácter personal. Puede cambiar su configuración siempre que lo desee. Dispone de más información en nuestra política de cookies"*. No se solicita la aceptación y en el acceso a la política de cookies figura "Error 404. Documento no encontrado".

En fecha 5 de diciembre de 2022, desde la Inspección de Datos se accede a la web https://www3.gobiernodecanarias.org/sanidad/scs/ del *SERVICIO CANARIO DE SALUD* verificando que dispone de un apartado de Política de Privacidad en el que se identifica como responsable del tratamiento y se incluye, entro otros, un enlace al Registro de Actividad del Tratamiento en el que se informa de la finalidad, base jurídica, destinatarios y conservación. Asimismo, se incluye un enlace para ejercitar los derechos de los interesados, dirección de correo electrónico del Delegado de Protección de Datos y un enlace a la web de la Agencia Española de Protección de Datos.

En el Registro de Actividades de Tratamiento figura el tratamiento HISTORIA CLINICA donde se informa de lo mencionado.

En el acceso a la web del *SERVICIO CANARIO DE SALUD* consta un aviso sobre cookies "E*l portal web del servicio canario de la salud utiliza cookies propias y de terceros para recopilar información que ayuda a optimizar su visita. Las cookies no se utilizan para recoger información de carácter personal. Usted puede permitir su uso o rechazarlo. También puede cambiar su configuración siempre que lo desee. Dispone de más información en nuestra política de cookies"*

En la Policita de cookies se informa sobre cookies técnicas y cookies analíticas en la que se indica "C*ookies analíticas para el seguimiento y análisis estadístico del comportamiento del conjunto de los usuarios. Si se desactivan estas cookies, el sitio web podrá seguir funcionando, sin perjuicio de que la información captada por estas cookies sobre el uso de nuestra web y sobre su contenido permite mejorar nuestros servicios"*

En fecha 9 de diciembre de 2022, desde la Inspección de Datos se accede a la web *CONSEJERÍA DE SANIDAD DEL GOBIERNO DE CANARIAS* verificando que genera tres cookies propias del Gobierno de Canarias. Una de ellas de sección y las otras, con fecha de expiración 10-12-2022 y 13-01-2024, son de Google Analytics. (D cookies).

En esta misma fecha, desde la Inspección de Datos se accede a la web del *SERVICIO CANARIO DE SALUD* verificando que genera cuatro cookies propias del Gobierno de Canarias. Con fechas de expiración: 9 y 10-12-2022 y 9 y 13-01-2024. Tres de ellas son de Google Analytics. (D cookies).

En las actuaciones AT/0724/2022 se procedió al traslado de la reclamación a la *CONSEJERIA DE SANIDAD DEL GOBIERNO DE CANARIAS* y al *SERVICIO CANARIO DE LA SALUD* siendo contestado por la *SERVICIO CANARIO DE LA SALUD* en los siguientes términos:

No consta que la reclamante haya efectuado una reclamación ante la *OFICINA DE SEGURIDAD (ODS) DEL ÁREA DE SERVICIOS ELECTROMÉDICOS Y DE LA INFORMACIÓN (ASEI)* ya que, como consta en el final del listado aportado por la reclamante, se informa que "*si alguno de los accesos incluidos en el informe pudiera haber sido indebido o ilícito puede presentar una reclamación con el fin de que la oficina de seguridad realice las verificaciones oportunas que ayuden a aclarar dicho acceso*".

Se ha aportado informe emitido por la ODS sobre la auditoría elaborada de los accesos realizados por *ATENCIÓN PRIMARIA Y ATENCIÓN ESPECIALIZADA EN HOSPITAL GENERAL DE FUERTEVENTURA* en el que se pone de manifiesto que los accesos fueron realizados por diez profesionales, de los cuales dos de ellos

accedieron a la historia para interesarse por el estado de salud de la reclamante ya que la identificaron en la lista de urgencia puesto que es profesional del Área de Anestesia y Reanimación (FEA).

Respecto a las cookies y la política de privacidad manifiestan que se encuentra trabajando en ello y aportan borradores al respecto. Dichos borradores son similares a los que se encuentran disponibles en la web del *SERVICIO CANARIO DE SALUD* en fecha 5 de diciembre de 2022, fecha en que se ha realizado el acceso desde la Inspección de Datos.

El *SERVICIO CANARIO DE SALUD* manifiesta y aporta escrito al respecto, que la *DIRECCIÓN DEL SERVICIO CANARIO DE LA SALUD*, órgano responsable de los tratamientos de Historia Clínica, tanto de Atención Primaria como de Atención Especializada, ha remitido escrito a todas las gerencias en los siguientes términos: "*La Agencia Española de Protección de Datos ha remitido, en un corto espacio de tiempo, varias reclamaciones relativas a accesos supuestamente indebidos a la historia clínica de pacientes por parte de personal del centro. La Instrucción n.º 4/10 de esta Dirección…. deja claro que en los órganos prestadores de servicios, el responsable del centro asistencial determinará qué unidades adoptarán, en nombre del responsable del tratamiento, las medidas necesarias para que el personal de cada unidad conozca, de forma comprensible, las normas de seguridad de los ficheros que afecten al desarrollo de sus funciones (apartado quinto). En este sentido, es importante que el personal que accede a la historia clínica conozca las responsabilidades disciplinarias…., accede a la historia clínica de un paciente por motivos no justificados. Del mismo modo se les recuerda que, ante cualquier indicio de accesos indebidos, la gerencia correspondiente deberá adoptar las medidas necesarias para depurar las responsabilidades administrativas o penales a que hubiere lugar".*

Con fecha 12 de diciembre de 2022 se remite requerimiento de información al *SERVICIO CANARIO DE SALUD* (en adelante SCS) y de la respuesta recibida se desprende:

<u>En relación con la Política de Seguridad</u>

El SCS ha aportado copia de la Política de Seguridad, cuya resolución de aprobación fue publicada en el Boletín Oficial de Canarias de fecha 13 de febrero de 2014, donde se establecen los criterios generales para los procedimientos de seguridad (Documento 1). Todo el personal debe ser informado de ella así como de la instrucción 04/2010 del Director del Servicio Canario de la Salud, relativa a la actuación del personal que, con motivo del desempeño de su puesto de trabajo, trata datos de carácter personal (Documento 2). Esta instrucción es de obligada lectura y cumplimiento para todo el personal que accede a los sistemas del SCS, entre ellos a la Historia clínica de los pacientes.

El SCS manifiesta que cuando se accede por primera vez, y de manera esporádica y aleatoria, salta un aviso en la pantalla recordando la existencia de dicha instrucción y con la recogida de la consiguiente aceptación por parte del personal de su lectura y compresión y aporta impresión de pantalla del mencionado aviso donde se informa: "*En los registros de este Servicio no consta que, como trabajador que presta su servicios en el SCS y en virtud de la normativa de Protección de Datos de carácter Personal, haya leído y aceptado la instrucción 04/2010 del Servicio Canario de la Salud relativa a la actuación del personal que trata datos de carácter personal. Por*

favor, para continuar, lea la instrucción y pulse en el botón correspondiente" (Documento 3).

El SCS ha aportado copia del Documento de Seguridad (Documento 4) en el que se recoge, entre otros aspectos, lo relativo a la identificación y autenticación de los usuarios con acceso a los sistemas de información y donde se indica que los responsables técnicos de cada aplicación podrán obtener el listado actualizado de usuarios así como sus perfiles de acceso. Asimismo, se indica que existirá relación actualizada de usuarios con acceso a los documentos no automatizados junto con sus derechos de acceso. Y, en lo relativo al control de accesos indica que los usuarios solo accederán a los recursos precisos para realizar su trabajo.

En caso de ficheros que contengan datos de nivel alto se establece, entre otros:

- Se guardará la información de los accesos que especifica el reglamento.
- Si el acceso es autorizado, se guardará la información que permita identificar el registro al que ha accedido el usuario.
- El Responsable de Seguridad controlará los mecanismos de este registro.

Medidas de seguridad del tratamiento HISTORIAS CLINICAS

El acceso a la historia clínica viene regulado en el Decreto 178/2005, de 26 de julio, por el que se aprueba el Reglamento que regula la historia clínica en los centros y establecimientos hospitalarios y establece el contenido, conservación y expurgo de sus documentos.

En el artículo 28 sobre *Procedimiento de constancia del acceso a la historia clínica y su uso*, en su apartado 5 establece: " *La informatización, en su caso, del procedimiento regulado en este artículo garantizará la seguridad, la identificación y autenticación de las personas que acceden a la información, así como un registro de dicho acceso, mediante la creación del correspondiente fichero, garantizando el cumplimiento de lo dispuesto en la legislación vigente en materia de protección de datos de carácter personal".*

El SCS manifiesta que dispone de un fichero que recoge la actividad de los usuarios en las distintas aplicaciones vinculadas a la historia clínica.

El SCS aporta el documento "*Normativa de control de acceso lógico"* donde se describe el procedimiento de control de acceso lógico que se aplica a todo el personal con acceso a la información custodiada por el SCS (Documento 6) y que, según figura en el mismo, recoge lo exigido en el Esquema Nacional de Seguridad. En el apartado 5 sobre Control de Acceso Lógico consta que además de la identificación y autenticación el sistema, basándose en los datos de identificación y autenticación, proporciona al usuario los privilegios necesarios para el acceso a los recursos.

El SCS también ha aportado copia del Análisis de Riesgo en el que figuran los tratamientos relativos a la Historia Clínica definidos como *Críticos* y manifiestan que se aplican las medidas de seguridad previstas en el Esquema Nacional de Seguridad. (Documento 7). A este respecto manifiestan que se encuentra en fase de implantación y adecuación al Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

En relación con la historia clínica del Hospital de Fuerteventura, han aportado auditoria de verificación de la Gestión de usuarios (Documento 8), así como la auditoría general de gestión de usuarios del SCS (Documento 9).

En relación con el Delegado de Protección de Datos

El SCS manifiesta que "*la Delegada de protección de Datos cumple sus funciones de conformidad con el artículo 39 del RGPD, principalmente asesora y supervisa el cumplimiento de la normativa vigente de protección de datos de oficio o bien a instancia del servicio implicado, valorando e informando de aquello que considera preciso para el correcto tratamiento de los datos de carácter personal".*

OCTAVO. Es objeto de este expediente la cuestión relativa a los posibles accesos indebidos a la historia clínica de la reclamante. La posible exigencia de responsabilidad por la utilización de cookies analíticas sin obtener el consentimiento de los usuarios en la web de la Consejería de Sanidad del Gobierno de Canarias, será objeto, en su caso, de un procedimiento diferente.

NOVENO: Con fecha 20 de abril de 2023**,** la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la parte reclamada, con arreglo a lo dispuesto en los artículos 63 y 64 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), por la presunta infracción del artículo 5.1.f) del RGPD y artículo 32 del RGPD, tipificada en el artículo 83.5 del RGPD.

DÉCIMO: Notificado el citado acuerdo de inicio conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), la parte reclamada, el 8 de mayo de 2023 presentó escrito de alegaciones en el que manifestaba que en relación a la infracción del artículo 5.1 f) del RGPD, para poder prestar una asistencia integral y lo más completa posible, se dispone de una historia clínica (en adelante HC) electrónica, a la que es preciso acceder mediante usuario y contraseña, dejando por ello registrados los logs de acceso a las distintas HC.

Actualmente no es técnicamente viable restringir el acceso a la HC de los usuarios únicamente a aquellos sanitarios que estén prestando una asistencia en el momento exacto a los pacientes, ya que pueden darse diversos casos en los que sea necesario acceder a especialidades, o pruebas solicitadas y revisadas por otro profesional o centro o que durante al asistencia se tenga que realizar una derivación a otro profesional. Es decir, para evitar comprometer la atención sanitaria, no es oportuno restringir completamente el acceso a la HC.

De las auditorías realizadas a 10 profesionales, se ha podido comprobar que efectivamente, 2 de esos accesos se han producido sin justificación asistencial, si bien no queda acreditado que la información a la que han accedido haya sido divulgada por ningún medio. Ambos profesionales indicaron que tuvieron conocimiento del ingreso de su compañera porque vieron su nombre en la lista de urgencias. Por ello, accedieron a su historia para saber si podían aportar algún conocimiento de su especialidad para ayudar en su mejoría.

En relación con la supuesta infracción del artículo 32 del RGPD, la entidad reclamada manifiesta que ha ido implementado las medidas de seguridad que se han ido determinando en función de los tratamientos realizados, valorando en todo caso las

posibles amenazas que pudiesen poner en riesgo la seguridad de la información tratada.

Siendo conscientes de que no existe la seguridad absoluta, el SCS ha ido adoptando medidas de seguridad y realizando labores de concienciación de su personal que han ido demostrando su eficacia hasta este caso particular.

Pruebas de esa revisión y adopción de nuevas medidas, están las indicadas en la publicación de la Instrucción 6/2023 y la elaboración de una nueva instrucción de acceso a la HC por parte del personal del SCS.

Así mismo, cuando se ha tenido conocimiento de estos posibles accesos indebidos, se ha realizado una auditoría interna dirigida a los profesionales implicados, a fin de que justificasen el motivo del acceso, y desde la Gerencia correspondiente, se están llevando a cabo actuaciones de instrucción disciplinaria para depurar las posibles responsabilidades.

La entidad reclamada concluye indicando que considerando que se trata de un hecho aislado producido desde la buena fe de los profesionales sanitarios para ayudar en la recuperación de su compañera, que se están tomando medidas adicionales necesarias tendentes a garantizar en mayor medida la confidencialidad de la información, solicita el archivo de las actuaciones.

UNDÉCIMO: Con fecha 9 de mayo de 2023, el instructor del procedimiento acuerda dar por reproducidos a efectos probatorios la reclamación interpuesta por ***A.A.A.*** y su documentación, los documentos obtenidos y generados durante la fase de admisión a trámite de la reclamación, y el informe de actuaciones previas de investigación que forman parte del procedimiento.

Asimismo, se da por reproducido a efectos probatorios, las alegaciones al acuerdo de inicio del procedimiento sancionador referenciado, presentadas por SERVICIO CANARIO DE LA SALUD, y la documentación que a ellas acompaña.

DUODÉCIMO: Con fecha 30 de mayo de 2023, se dicta propuesta de resolución en la que se propone que por la Directora de la Agencia Española de Protección de Datos se dirija un apercibimiento a SERVICIO CANARIO DE LA SALUD, con NIF Q8555011I, por cada una de las dos infracciones cometidas, uno por la infracción del artículo 5.1.f) del RGPD y otro por la infracción del artículo 32 del RGPD, tipificadas ambas en el artículo 83.5 del RGPD.

DÉCIMOTERCERO: Con fecha 9 de junio de 2923 se reciben las siguientes alegaciones por parte de la entidad reclamada en respuesta a la propuesta de resolución:

"1º.- Atendiendo a lo establecido en el art. 5.1 del RGPD, se determina que los datos 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»), se considera que lo que

se está afirmando es que el SCS no hace un tratamiento de datos que garantice la aplicación de los principios recogidos en el mencionado precepto, no estando conformes con dicho extremo.

Teniendo en cuenta el tipo de servicios que presta el SCS a los usuarios, y para que la asistencia sanitaria sea lo más integral y completa posible, se dispone de una historia clínica (en adelante HC) electrónica a la que pueden acceder los profesionales sanitarios, mediante usuario y contraseña, y cuyos logs de acceso son registrados. Actualmente y debido a la actividad del SCS, no es técnicamente viable restringir el acceso a la HC de los usuarios únicamente a aquellos sanitarios que estén prestando una asistencia en el momento exacto a los pacientes, ya que pueden darse diversos casos en los que sea necesario acceder a especialidades, o pruebas solicitadas y revisadas por otro profesional o centro o que durante la asistencia se tenga que realizar una derivación a otro profesional.

No obstante, en aras del ejercicio de la responsabilidad proactiva, el SCS está elaborando una instrucción para intentar acotar lo máximo posible los accesos a la HC, partiendo de la premisa anteriormente expuesta, de que no es posible disponer de un acceso restringido a la HC para garantizar la agilidad con que deben desarrollarse las prestaciones asistenciales.

En esta nueva instrucción de la Dirección del SCS, se están dando indicaciones para implementar la justificación de accesos a la HC cuando, por ejemplo, no es un usuario perteneciente al cupo del profesional o bien no está siendo atendido por este en urgencias o en alguna especialidad (se adjunta último borrador de la instrucción de accesos a la HC como Doc. 1), tal y como solicitó la reclamante a algún compañero para conocer estados de pruebas o intentar agilizar trámites administrativos.

A parte de esto, por parte del SCS se realizan labores de concienciación y formación al personal y se ha publicado recientemente una actualización de la anterior Instrucción 4/2010, Instrucción Núm. 6/2023 de la Directora del Servicio Canario de la Salud, relativa al tratamiento de datos personales efectuado por el personal del Servicio Canario de la Salud, en el desempeño de su puesto de trabajo, la cual ha sido difundida entre el personal y se encuentra accesible en la intranet (se acompaña como Doc. 2).

Por lo expuesto, no se considera adecuado afirmar que

a) El tratamiento de datos personales, se está realizado, vulnerando los principios y garantías establecidos en el artículo 5 del Reglamento (UE) 2016/679, ya que el responsable del tratamiento, el SCS, ha adoptado medidas tendentes a garantizar la confidencialidad de los datos contenidos en la HC electrónica, con diversos avisos al iniciar la sesión, concienciando al personal sobre la necesidad de mantener la confidencialidad y acceder a los estrictamente imprescindibles para el desarrollo de sus funciones, etc., medidas que además están siendo reforzadas actualmente con la nueva Instrucción de Acceso a la HC en vías de aprobación.

Según informa la AEPD, la reclamante afirma que la información sanitaria relativa a su persona ha sido divulgada a terceros por los profesionales que accedieron a su HC, si bien no queda acreditado este hecho más allá de la aseveración de parte y sin constatación de este hecho por parte de los profesionales al ser requeridos en la auditoría dirigida que se les realizó, por lo que dicha afirmación no queda probada y no debe tenerse en consideración.

2º.- Por otro lado, se sanciona por incumplimiento del artículo 32 que determina 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: […]

b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;"

Pues bien, el SCS ha ido implementado las medidas de seguridad que se han ido determinando en función de los tratamientos realizados, valorando en todo caso las posibles amenazas que pudiesen poner en riesgo la seguridad de la información tratada.

En los análisis realizados siempre se ha tenido y se tiene en cuenta el factor humano como una de las amenazas presentes en cualquier tratamiento; aplicándose las contramedidas oportunas para mitigar dicho riesgo que, hasta la fecha han resultado efectivas, si bien con este caso puntual se ha demostrado que no son infalibles.

*Por tanto, determinar que no se han aplicado medidas técnicas y organizativas para garantizar la confidencialidad de la información y sancionar por ello, se considera excesivo, puesto que si se han establecido medidas en base a los riesgos analizados, si bien, como se indicó anteriormente, se han demostrado que no son invulnerables. Siendo conscientes de que no existe la seguridad absoluta, el SCS ha ido adoptando medidas de seguridad y realizando labores de concienciación de su personal que han ido demostrando su eficacia hasta este caso particular, entre otras, con la publicación de la Instrucción 6/20***PS/00587/2021,** un PS abierto al SERVICIO MADRILEÑO DE SALUD.

23 y la elaboración de una nueva instrucción de acceso a la HC por parte del personal del SCS.

3º.- Se aplica una doble sanción para un mismo hecho, toda vez que se propone sancionar como muy grave la infracción del artículo 5.1.f) del RGPD y como grave la infracción del artículo 32 del RGPD, entre cuyas medidas ya se encuentra garantizar la confidencialidad de la información, por lo que se está duplicando la sanción del supuesto hecho cometido.

Por todo lo expuesto, y considerando que se trata de un hecho aislado producido desde la buena fe de los profesionales sanitarios para ayudar en la recuperación de su compañera, que se están tomando medidas de refuerzo tendentes a garantizar en mayor medida la confidencialidad de la información, SOLICITAMOS el archivo de las actuaciones."

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: Se han producido accesos indebidos a la historia clínica del reclamante, lo cual hace posible la revelación de tales datos de carácter personal, a terceros pese a no contar con el consentimiento del titular de los mismos.

SEGUNDO: La entidad reclamada ha aportado Informe emitido por la Oficina de Seguridad (ODS) del Área de Servicios Electromédicos y de la Información (ASEI) sobre la auditoría elaborada de los accesos realizados por Atención Primaria y Atención Especializada en Hospital General de Fuerteventura en el que se pone de manifiesto que los accesos fueron realizados por diez profesionales, de los cuales dos de ellos accedieron a la historia para interesarse por el estado de salud de la reclamante ya que la identificaron en la lista de urgencia puesto que es profesional del Área de Anestesia y Reanimación (FEA).

FUNDAMENTOS DE DERECHO

I

De acuerdo con lo dispuesto en los artículos 58.2 y 60 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD), y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 y 68.2 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD) es competente para iniciar y resolver este procedimiento la Directora de la Agencia Española de Protección de Datos.

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

II

Sobre el dato de salud señala el considerando 35 del RGPD:

“Entre los datos personales relativos a la salud se deben incluir todos los datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro. Se incluye la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia, de conformidad con la Directiva 2011/24/UE del Parlamento Europeo y del Consejo; todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro.”

Por su parte, el artículo 4 del RGPD define:

“2) «tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;”

7) «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros;

10) «tercero»: persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado;”

III

El tratamiento de datos de las historias clínicas se encuentra regulado en la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

Su artículo 3 señala:

"Historia clínica: el conjunto de documentos que contienen los datos, valoraciones e informaciones de cualquier índole sobre la situación y la evolución clínica de un paciente a lo largo del proceso asistencial".

En el artículo 16, se establecen los usos de la historia clínica:

"1. La historia clínica es un instrumento destinado fundamentalmente a garantizar una asistencia adecuada al paciente. Los profesionales asistenciales del centro que realizan el diagnóstico o el tratamiento del paciente tienen acceso a la historia clínica de éste como instrumento fundamental para su adecuada asistencia.

2. Cada centro establecerá los métodos que posibiliten en todo momento el acceso a la historia clínica de cada paciente por los profesionales que le asisten."

IV

Los principios relativos al tratamiento de datos de carácter personal, se regulan en el artículo 5 del RGPD donde se establece que *"los datos personales serán:*

"a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);

b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);

c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);

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»);

e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que

impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);

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

El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).”

V

En el presente caso se presenta reclamación por los accesos indebidos a la historia clínica y la revelación a terceros del diagnóstico de la parte reclamante.

En relación con los accesos indebidos la entidad ha aportado:

- Informe emitido por la Oficina de Seguridad (ODS) del Área de Servicios Electromédicos y de la Información (ASEI) sobre la auditoría elaborada de los accesos realizados por Atención Primaria y Atención Especializada en Hospital General de Fuerteventura en el que se pone de manifiesto que los accesos fueron realizados por diez profesionales, de los cuales dos de ellos accedieron a la historia para interesarse por el estado de salud de la reclamante ya que la identificaron en la lista de urgencia puesto que es profesional del Área de Anestesia y Reanimación (FEA).
- No consta que la reclamante haya efectuado una reclamación ante la ODS.

En relación con la Seguridad de los tratamientos la entidad ha aportado

- Política de Seguridad, cuya resolución de aprobación fue publicada en el Boletín Oficial de Canarias de fecha 13 de febrero de 2014.
- Instrucción 04/2010 del Director del ***SERVICIO CANARIO DE LA SALUD***, relativa a la actuación del personal que, con motivo del desempeño de su puesto de trabajo, trata datos de carácter personal.
- Documento de seguridad.
- Decreto 178/2005, de 26 de julio, por el que se aprueba el Reglamento que regula la historia clínica en los centros y establecimientos hospitalarios y establece el contenido, conservación y expurgo de sus documentos.
- Normativa de control de acceso lógico de conformidad con el Esquema Nacional de Seguridad.
- Análisis de Riesgo en el que figuran los tratamientos relativos a la Historia Clínica definidos como *Críticos* y manifiestan que se aplican las medidas de seguridad previstas en el Esquema Nacional de Seguridad.

Tal y como se ha indicado en el fundamento de derecho III, de la lectura del artículo 16 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica se infiere con claridad que, si bien la historia clínica es el instrumento para

prestar la asistencia sanitaria al paciente, lo que debe quedar debidamente garantizado, también lo es el hecho de que sólo puede producirse el acceso a la historia clínica por los profesionales que le asisten, no con carácter general, sino con carácter particular realizando la diagnosis o el tratamiento del paciente.

Pese a las medidas técnicas y organizativas implantadas no ha impedido el acceso a la historia clínica de un paciente, por terceros, lo cual denota la ausencia de medidas que garanticen 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.

Y en cuanto al principio de protección de datos desde el diseño, el RGPD exige en su artículo 25:

"1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados"

Por ello, se considera que tales hechos suponen una vulneración de la confidencialidad, y con ello contraviene el artículo 5.1 f) del RGPD, que rige el principio de integridad y confidencialidad, ya que se han producido unos accesos indebidos a la historia clínica, perdiendo los datos de salud que la misma contiene su confidencialidad, al permitirse el acceso por terceros que no estaban legitimados para ello.

El criterio de la AEPD en relación con este tipo de accesos no autorizados tiene un precedente claro, producido en un procedimiento sancionador tramitado tras la entrada en vigor del RGPD. Se trata del expediente referencia PS/00250/2021, en que se sancionó al SERVICIO EXTREMEÑO DE SALUD por un problema idéntico al que nos ocupa en este expediente. En la narración de los hechos figura:

"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."

Por lo tanto, esta Agencia considera que los hechos denunciados consistentes en la revelación de los datos médicos del reclamante a personas no autorizadas constituyen una infracción del artículo 5.1.f) del RGPD

VI

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

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

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

A efectos del plazo de prescripción, el artículo 72.1 a) de la LOPDGDD señala que "*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".

VII

Por otro lado, la seguridad en el tratamiento de datos personales viene regulada en el artículo 32 del RGPD donde se establece 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 apro-*

piadas 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."*

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."

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

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

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

A efectos del plazo de prescripción, el artículo 73.g) de la LOPDGDD, bajo la rúbrica "Infracciones consideradas graves dispone:

"En función del artículo 83.4 del Reglamento (UE) 2016/679 se considerarán graves y prescribirán a los dos años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel, y en particular los 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."

VIII

En este supuesto, esta Agencia ha constatado que las medidas de seguridad de la entidad reclamada no son adecuadas, lo que constituye por parte de la entidad reclamada, infracción a lo dispuesto en el artículo 32 del RGPD.

La falta de adopción de medidas para garantizar el principio de confidencialidad hace que no pueda considerarse que existan medidas que aporten un nivel de protección adecuado a los riesgos existentes, esto es así porque la política de Seguridad establecida se fundamenta en una resolución de fecha 13 de febrero de 2014, una Instrucción del año 2010 dictada por el Director del ***SERVICIO CANARIO DE LA SALUD***, y un Decreto 178/2005, de 26 de julio, por el que se aprueba el Reglamento que regula la historia clínica en los centros y establecimientos hospitalarios y establece el contenido, conservación y expurgo de sus documentos, todas ellas son normas previas a la normativa vigente en materia de protección de datos, cuyo eje parte del RGPD 2016/679, en vigor desde el 25 de mayo de 2018.

Por lo tanto, al no adoptar las medidas de seguridad necesarias para garantizar la protección de los datos de carácter personal de los pacientes de este servicio de salud, se considera que se ha vulnerado el artículo 32 del RGPD.

IX

En conclusión, ha de señalarse que de conformidad con las evidencias de las que se dispone, se considera que la entidad reclamada ha tratado datos personales del reclamante, su historia clínica y diagnóstico, permitiendo su acceso sin adoptar las medidas técnicas u organizativas apropiadas, lo cual implica una vulneración del artículo 5.1 f) del RGPD, ni tampoco se han adoptado las medidas de seguridad exigidas por la normativa en materia de protección de datos de carácter personal, dando lugar a una vulneración del artículo 32 del RGPD.

Así las cosas, esta Agencia considera que la entidad reclamada ha infringido los artículos 5.1 f) y 32 del RGPD, al violar el principio de integridad y confidencialidad, así como no adoptar las medidas de seguridad necesarias para garantizar la protección de los datos de carácter personal de los pacientes de este servicio de salud.

Por lo tanto, este procedimiento concluye con la imposición de dos sanciones por estos hechos: una por la vulneración del artículo 5.1.f) RGPD, y otra por el artículo 32 RGPD.

X

El artículo 58.2 del RGPD dispone lo siguiente: "*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;

d) ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado;

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;

XI

El artículo 83 "*Condiciones generales para la imposición de multas administrativas*" del RGPD en su apartado 7 establece:

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

Asimismo, el artículo 77 "*Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento*" de la LOPDGDD, dispone, conforme a la redacción vigente en el momento de producirse los hechos, lo siguiente:

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

d) Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas.

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."

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: DIRIGIR a ***SERVICIO CANARIO DE LA SALUD***, con NIF ***Q8555011I***, por una infracción del artículo 5.1.f) del RGPD y artículo 32 del RGPD, tipificada en el artículo 83.5 y 83.4 del RGPD respectivamente, una sanción de apercibimiento por cada infracción cometida.

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

TERCERO: PROPONER el inicio de actuaciones disciplinarias contra los facultativos que accedieron a la historia clínica del reclamante.

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

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

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

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

938-181022

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