Procedimiento Nº: PS/00078/2019
938-0419

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: D.ª ***A.A.A.***(en adelante, la reclamante) presenta el 28/09/2018 ante la Agencia Española de Protección de Datos (en adelante AEPD) una reclamación en la que expone que D.ª ***B.B.B.***, con NIF ******NIF.2*** -Clínica de Fisioterapia Santa Fe- (en adelante, la reclamada) ha remitido a una dirección de correo electrónico que no le pertenece sus informes médicos, en los que constan sus datos personales.

Añade que el documento de protección de datos que la reclamada le dio a firmar mencionaba únicamente la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, sin aludir en ningún caso a las disposiciones del Reglamento General de Protección de Datos (UE) 2016/679, lo que le hace sospechar que la documentación que firmó "*no cumple enteramente con la norma vigente".*

Acompaña al escrito de reclamación copia de los documentos siguientes:

- Impresión del correo electrónico que envió a la Clínica de Fisioterapia Santa Fe el 07/09/2018 en el que se incluía, como archivo adjunto, el informe médico que le habían solicitado.
- Impresión del correo electrónico que la reclamada envió a un destinatario incorrecto.
- Hoja de reclamación de la Dirección General de Comercio, Consumo y Cooperación Económica de la Consejería de Trabajo e Industria de la Junta de Andalucía, cumplimentada y firmada por la reclamante, que lleva sello de presentación ante la Delegación Provincial del Servicio de Consumo de Granada.

SEGUNDO: A la vista de los hechos expuestos, la AEPD, conforme a lo establecido en el artículo 9.4 del Real Decreto-Ley 5/2018, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos, en el ámbito del expediente E/7715/2018, mediante escrito de fecha 22/10/2018, dio traslado de la reclamación a la reclamada para que procediera a su análisis, informara a esta Agencia, en el plazo de un mes, de las causas que a su juicio habían provocado la incidencia que originó la reclamación y comunicara a la reclamante las medidas adoptadas al respecto.

Obra en el expediente la documentación que acredita que la reclamada recibió el 25/10/2018 el escrito de la AEPD en el que se le daba traslado de la reclamación. La reclamada respondió al requerimiento informativo de la Agencia en escrito de fecha 13/12/2018, al que anexó una copia de la carta que envió a la reclamante explicándole el origen de los hechos -que se debieron a un error al escribir su dirección electrónica- y que habían resultado infructuosos los intentos efectuados para contactar con la propietaria de la dirección electrónica a la que, por error, se envió el escrito que iba dirigido a ella y con el que se anexaba su informe médico. En ese escrito dirigido a la reclamante la reclamada reiteró las disculpas que ya le había ofrecido cuando el informe le fue entregado personalmente ante la Policía Municipal, después de cumplimentar un formulario de Reclamaciones de Consumo. La reclamada acredita a través de un certificado de Correos el envío por burofax a la reclamante del escrito mencionado.

La AEPD notificó a la reclamante las actuaciones realizadas en escrito de fecha 22/10/2018 que consta recibido el 31/10/2018.

De conformidad con lo dispuesto en el artículo 65.5 de la LOPDGDD, en fecha 21/12/2018, la AEPD acordó admitir a trámite la reclamación y notificó tal acuerdo a la reclamante.

En el marco del expediente de referencia E/00458/2019, a tenor de lo prevenido en el artículo 58.1 del RGPD y 67 de la LOPDGDD, se practicaron actuaciones de investigación previa dirigidas al esclarecimiento de los hechos a cuyo fin se solicitó información adicional a la reclamada.

Se transcribe a continuación el Informe de Actuaciones Previas de inspección E/00458/2019:

<<

1 *Con fecha 7 de septiembre de 2018 la denunciante remite a la Clínica de Fisioterapia y Rehabilitación Santa Fe el informe médico solicitado en visita presencial para determinar el tratamiento adecuado.*

1. *Con fecha 14 de septiembre de 2018 la clínica envió a una dirección de correo errónea el tratamiento correspondiente a la interesada.*

2. *En los escritos recibidos, se observa que la diferencia entre la dirección de correo de la interesada y la dirección de correo errónea, hay una variación en una letra. En vez de remitir la información a la dirección* ******EMAIL.1,*** *se envió a* ******EMAIL.2***

3. *De esta dirección errónea no se recibido en la dirección de correo electrónico de la clínica informe de error por parte del servidor de destino, lo que quiere decir que es una dirección de correo válida y que el informe con el tratamiento ha sido entregado en esta dirección de correo.*

4. *Con fecha 28 de enero de 2019 se recibe en esta Agencia, con número de registro* ******REGISTRO.1****, escrito procedente de la Clínica de Fisioterapia y Rehabilitación Santa Fe, donde se manifiesta que la dirección de correo de la interesada se recabo de palabra. Manifiestan en este escrito que han intentado ponerse en contacto con la persona a la que corresponde esta dirección de*

correo errónea sin éxito. También han buscado en redes sociales con el nombre de "Rose Ish" encontrando una referencia con este nombre en Facebook pero sin identificación, biografía, fotos, ni amigos.

Así mismo adjuntan la autorización para el tratamiento de datos personales firmada por la denunciante de 7 de septiembre de 2018 recogiendo la aplicación de la normativa de la Ley 15/1999. También adjuntan impresos actualizados al Reglamento (EU) 679/2016. >>

TERCERO: Con fecha 5 de marzo de 2019, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la reclamada por la presunta infracción de los artículos 13 y 32 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27/04/2016, 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 (Reglamento General de Protección de Datos, en adelante RGPD)

CUARTO: El acuerdo de inicio del procedimiento sancionador PS/78/2019 fue notificado a la reclamada en fecha 11/03/2019.

La reclamada no formuló alegaciones al acuerdo de inicio del expediente sancionador. No se tiene noticia en este organismo de la entrada de ningún escrito de la reclamada a través del cual dé cumplimiento al trámite de alegaciones que le otorga la Ley.

El artículo 64.2.f) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP) señala que, en caso de no efectuar alegaciones en el plazo previsto sobre el contenido del acuerdo de iniciación, éste podrá ser considerado propuesta de resolución cuando contenga un pronunciamiento preciso acerca de la responsabilidad imputada.

Habida cuenta de que el plazo fijado en la LPACAP para hacer alegaciones al acuerdo de inicio del expediente sancionador se superó con creces sin que la reclamada hubiera evacuado el trámite, y, puesto que dicho acuerdo contenía –tal y como exige el artículo 64.2.f) de la LPACAP- "*un pronunciamiento preciso acerca de la responsabilidad imputada",* hemos de concluir que, en el asunto que nos ocupa, el referido acuerdo de inicio se considera propuesta de resolución, de manera que la instructora del expediente lo eleva sin más trámites al órgano competente para resolver (ex artículo 88.7 LPACAP).

En el presente procedimiento han quedado acreditados los siguientes,

HECHOS

1º. La reclamante, D. ª ***A.A.A.***, con NIF ******NIF.1,*** y titular de la dirección electrónica "******EMAIL.1"*** denuncia que la Clínica de Fisioterapia Santa Fe -nombre comercial bajo el que opera la reclamada en calidad de empresario autónomo- envió un informe médico con sus datos personales a una dirección electrónica que no le pertenece. Añade que la documentación que firmó en esa empresa, relativa a protección de

datos, no se adaptaba a la normativa vigente pues hacía mención aún a la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal.

2º: Obran en el expediente copias de los siguientes correos electrónicos

1. Enviado el 07/09/2018 a las 19:32 horas desde ***EMAIL.1 a ***EMAIL.3 con el texto siguiente:
   "(…) Según lo acordado remito informa médico….".
   Se anexa con ese correo un documento en pdf denominado "***DOCUMENTO.1f".
2. Enviado el 14/09/2018 a las 8:47 horas desde la dirección ***EMAIL.3 a la dirección ***EMAIL.2. Como "*Asunto*" del email figura "*informe*". El correo está firmado por la reclamada (identificada por su nombre y dos apellidos) e inmediatamente debajo la indicación "*Fisioterapeuta*" y el número de colegiado.

3º: La reclamada ha reconocido que, por "*un error*", remitió el informe médico de la reclamante a una dirección electrónica que no fue la que ella le había facilitado. El error consistió -según sus explicaciones- en escribir como dirección electrónica de destino "***NOMBRE.2***" en lugar de "***NOMBRE.1***", que era la dirección correcta y la que reconoce que la reclamante le había facilitado

4º: La reclamada informó a la AEPD en su escrito de 13/02/2019, en el que respondió al requerimiento informativo de la Agencia en el E/7715/2018, que "*Desde la detección del error se ha tomado la decisión de enviar los informes médicos de los pacientes que lo soliciten por medios electrónicos sin incluir sus datos personales identificativos".*

5º: La reclamada, en su escrito de 28/01/2019, en el marco del E/4355/2019, reconoce que la información que facilitó a la reclamante al recabar sus datos personales no estaba actualizado a la normativa vigente y hacía referencia todavía a la Ley Orgánica 15/1999. Aporta una copia del documento, que aparece firmado por la reclamante el 07/09/2018 en el que se informa de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición y de la identidad del responsable.

6º: La reclamada aportó con su escrito de 28/01/2019 de respuesta al requerimiento de la inspección de datos, una copia del documento informativo que en calidad de responsable del tratamiento se proporciona, en la actualidad, a las personas de las que recaba datos personales.

El documento está adaptado al Reglamento UE 2016/679 y en él se facilita información acerca de la identidad del responsable del tratamiento; de la finalidad del tratamiento; de la base jurídica del tratamiento; de las consecuencias de no facilitar sus datos personales; de la posibilidad de comunicarlos al personal sanitario que trabaja para el responsable o a Administraciones Públicas con competencia en la materia; del plazo para su supresión; de la posibilidad de ejercitar los derechos de acceso, rectificación, suspensión, limitación de tratamiento u oposición al tratamiento y a presentar una reclamación ante la autoridad de control.

Además, la reclamada aportó con su escrito de 28/01/2019, un formulario para que los pacientes puedan ejercitar ante ella los derechos reconocidos en los artículos 15 a 22 del RGPD.

FUNDAMENTOS DE DERECHO

I

En virtud de los poderes que el artículo 58.2 del Reglamento 2016/679 (UE) de protección de datos (en adelante RGPD) reconoce a cada autoridad de control, y según lo establecido en los artículos 47 y 48.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantías de los derechos digitales (LOPDGDD), la Directora de la Agencia Española de Protección de Datos es competente para resolver este procedimiento.

II

El artículo 5 del RGPD, *"Principios relativos al tratamiento",* menciona entre ellos los de *"transparencia"* e *"integridad y confidencialidad".* El precepto establece:

"Los datos personales serán:

a) tratados de manera lícita, leal y transparente en relación con el interesado (<<licitud, lealtad y transparencia>>)

(…)

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

El artículo 13 del RGPD, bajo la rúbrica *"Información que deberá facilitarse cuando los datos personales se obtengan del interesado",* dice:

"1. Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:

a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;

b) los datos de contacto del delegado de protección de datos, en su caso;

c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;

d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;

e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;

f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.

2. Además de la información mencionada en el apartado 1, el responsable del

tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:

a) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;

b) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;

c) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;

d) el derecho a presentar una reclamación ante una autoridad de control;

e) si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos;

f) la existencia de decisiones automatizas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

3. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2.

4. Las disposiciones de los apartados 1, 2 y 3 no serán aplicables cuando y en la medida en que el interesado ya disponga de la información.>>

La vulneración del deber de informar al interesado de quien se recaben datos personales en los términos que exige el artículo 13 del RGPD se encuentra tipificada en el artículo 83.5. del RGPD, precepto que establece:

"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:

(…)

los derechos de los interesados a tenor de los artículos 12 a 22;"

La LOPDGDD, a efectos de prescripción, califica en su artículo 72.1.h como infracción muy grave la omisión del deber de informar al afectado acerca del tratamiento de sus datos personales conforme a lo dispuesto en los artículos 13 y 14 del Reglamento UE 2016/679.

A su vez, el artículo 32 del RGPD, relativo a la *"Seguridad de los datos",* señala*:*

"1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de

probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) la seudonimización y el cifrado de datos personales;

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

c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

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

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

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

La vulneración de la obligación que impone el artículo 32 del RGPD se encuentra tipificada en el artículo 83.4 del RGPD, precepto que establece:

"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 … 25 a 39…"*

La LOPDGDD, a efectos de prescripción, califica en su artículo 73 f) como infracción grave la falta de adopción de aquellas medidas técnicas y organizativas que resulten aplicables 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.

III

Se atribuye a la reclamada en este expediente sancionador la infracción de los artículos 13 y 32 del RGPD. Las conductas en las que se concreta esta infracción consistieron, por una parte, en no facilitar a la reclamante al tiempo de recabar sus datos personales la información a la que se refiere el artículo 13 del RGPD, y por otra,

en haber omitido las medidas de seguridad que estaba obligada a adoptar, al amparo del artículo 32 del RGPD, cuando remitió por correo electrónico un informe médico de la reclamante con datos de salud a una dirección que resultó ser errónea.

a.- Respecto a la infracción del artículo 13 RGPD, la reclamada ha reconocido que la información que facilitó a la reclamante no se ajustaba a la normativa vigente. Ha aportado la copia del documento informativo que la reclamante firmó en septiembre de 2018 (vigente el RGPD desde el 25/05/2018) cuyo contenido se ajustaba a la LOPD y no al Reglamento 2016/679.

Así pues, consta en el expediente plenamente acreditada la vulneración por la reclamada, en relación con el tratamiento de los datos personales de la reclamante, del artículo 13 del RGPD.

Ahora bien, debe subrayarse que la reclamada ha aportado a esta Agencia en la misma fecha el nuevo documento informativo que facilita a los terceros de quienes recoge datos personales. Como se detalla en el Hecho Probado 6º el documento informativo cumple las exigencias del artículo 13 del RGPD.

b.-Por lo que respecta a la infracción del artículo 32 del RGPD de la que se responsabiliza a la reclamada ha quedado plenamente acreditada a tenor de los documentos que obran en el expediente y de lo manifestado por ella en su respuesta a las solicitudes informativas que se le hicieron.

En el Hecho probado segundo se transcribe el correo electrónico que la reclamada envió el 14/09/2018, con el que incorporaba anexo el informe médico que la reclamante le había trasladado días antes, el 07/09/2018, también como documento anexo. Se comprueba en este email que la dirección electrónica de la reclamante es "***EMAIL.1" mientras que la reclamada envió el suyo a una dirección distinta "***EMAIL.2**

Los documentos que obran en el expediente y las declaraciones de la reclamada evidencian que ésta no había adoptado ninguna medida que garantizara la integridad de los datos personales que trata, en particular con ocasión de su comunicación a través de medios electrónicos.

La reclamada, en respuesta a la solicitud que le hizo la AEPD antes de la apertura del acuerdo de inicio del expediente para que informara sobre las medidas había adoptado para evitar que en el futuro se produzcan hechos análogos, informó en escrito de 13/02/2019 que "*Desde la detección del error se ha tomado la decisión de enviar los informes médicos de los pacientes que lo soliciten por medios electrónicos sin incluir sus datos personales identificativos".*

A propósito de la medida que dice haber adoptado hemos de advertir que no parece que tal decisión signifique una auténtica garantía de la integridad de los datos objeto de tratamiento. Por una parte, porque, aunque en el email no se identifique e al destinatario por su nombre, apellidos y NIF, en muchas ocasiones las direcciones de correo incorporan alguno o algunos de esos datos. Por otra, porque, además de que los documentos del informe medico suelen incluir esos datos, el concepto de dato

personal no se circunscribe a nombre, apellidos y NIF. El artículo 4.1) del RGPD entiende por dato personal "*toda información sobre una persona física identificada o identificable ("el interesado"); se considera persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona".*

Por tanto, en relación a la infracción del artículo 32 del RGPD, tipificada en el artículo 83.4 de esa norma, de la que es responsable la reclamada, ésta no ha acreditado haber adoptado medida alguna con virtualidad para garantizar el cumplimiento de las obligaciones que le impone el precepto vulnerado.

IV

El artículo 58 del RGPD, "*Poderes*", dice:

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

(…)

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

(...)

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 del caso particular

(…)"

Pese a que los artículos 83.5 y 83.4 RGPD prevén una sanción de multa administrativa, respectivamente, para las infracciones de los artículos 13 y 32 del RGPD de las que se responsabiliza a la reclamada, el artículo 58.2 del RGPD contempla la posibilidad de sancionar las infracciones del presente Reglamento con *"apercibimiento".*

Sobre la procedencia de optar por la sanción de apercibimiento y no por la multa administrativa prevista en los artículos 83.4 y 5 RGPD, cabe mencionar, como elemento que permite una interpretación auténtica de la norma, el Considerando 148 del Reglamento 2016/679 que contiene esta reflexión:

"En caso de infracción leve, o si la multa que probablemente se impusiera constituyese una carga desproporcionada para una persona física, en lugar de sanción mediante multa puede imponerse un apercibimiento. Debe no obstante prestarse especial atención a la naturaleza, gravedad y duración de la infracción, a su carácter intencional, a las medidas tomadas para paliar los daños y perjuicios sufridos, al grado de responsabilidad o a cualquier infracción anterior pertinente, a la forma en que la autoridad de control haya tenido conocimiento de la infracción, al cumplimiento

de medidas ordenadas contra el responsable o encargado, a la adhesión a códigos de conducta y a cualquier otra circunstancia agravante o atenuante" (El subrayado es de la AEPD)

A efectos de determinar la sanción que es procedente imponer por la infracción de los artículo 13 y 32 del RGPD de la que se responsabiliza a la reclamada, se toman en consideración factores tan relevantes como el carácter de empresario autónomo de la persona física responsable del tratamiento; la colaboración que ha prestado a esta Agencia, pues respondió con prontitud a los dos requerimientos que se le hicieron; las medidas que adoptó ante la situación irregular causada -nos referimos al envío a la reclamante mediante burofax de fecha 26/11/2018 de una carta en la que reconoció el error cometido y le pidió disculpas, la adecuación de su política de protección de datos a las previsiones del artículo 13 del RGPD, norma vigente desde el 25/05/2018 y, por tanto, vigente cuando la reclamante acudió al establecimiento de la reclamada y facilitó sus datos personales-; la rectificación efectuada en sus ficheros del dato inexacto -la dirección email de la reclamante-; las acciones que ha desplegado para tratar de localizar al titular de la dirección electrónica a la que por error envió el informe médico de la reclamante junto con sus datos identificativos -de la que es exponente su afirmación de que la búsqueda se ha concretado únicamente en una referencia hallada en Facebook a "******REFERENCIA.1"*** sin perfil, ni historia ni contacto o la decisión que, dice, ha adoptado desde la detección de estos hechos de no incluir datos personales cuando los pacientes soliciten la remisión de sus informes médicos por medios electrónicos, conduce a concluir que la sanción que procede imponer por las infracciones del RGPD cuya responsabilidad se atribuye a la reclamada, sea la de apercibimiento y no la de multa prevista en los artículos 83.4 y 83.5 RGPD, por ser más s acorde con el espíritu del RGPD a la luz del Considerando 148.

Adicionalmente, al amparo de la previsión del artículo 58.2 del RGPD que reconoce a las autoridades de control diversos poderes correctivos, y en particular del apartado d) del precepto, se estima procedente ordenar a la reclamada que adopte las medidas técnicas y organizativas que sean apropiadas para garantizar un nivel de seguridad adecuado al riesgo que entraña el tratamiento de datos que realiza de conformidad con el artículo 32 del RGPD. La adopción de estas medidas deberá acreditarse ante esta Agencia en el plazo de un mes desde la fecha en la que la resolución en la que se acuerdan sea ejecutiva.

A propósito de esta cuestión la Agencia reitera que, como explicó en el acuerdo de inicio del expediente, un tipo de medida adoptada en casos similares que ha demostrado tener consistencia para cumplir la finalidad perseguida es asignar al paciente una clave o contraseña que sólo él conoce. Esa clave o contraseña es remitida al paciente por otro medio distinto del correo electrónico, debiendo introducirla el paciente para la lectura de los mensajes que reciba vía email.

Se recuerda, asimismo, que, llegado el caso, incumbe al responsable del tratamiento la carga de demostrar la virtualidad de las medidas adoptadas para el cumplimiento de los fines perseguidos y que deberá tener en cuenta -pues parece desprenderse otra cosa del tenor de la respuesta a la solicitud informativa de esta Agencia- que la condición de dato personal no se predica únicamente del NIF, el nombre y los apellidos. Nos remitimos sobre el particular a la definición de dato

personal que ofrece el artículo 4. 1 del RGPD.

En relación con las medidas correctivas del artículo 58.2 RGPD que se acuerda imponer a la reclamada en el procedimiento sancionador que nos ocupa, debe recordarse que el Reglamento (UE) 2016/679 sanciona *"El incumplimiento de las resoluciones de la autoridad de control a tenor del artículo 58, apartado 2"* con multa administrativa de 20.000.000 de euros 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 (artículo 83.6 RGPD)

Por lo tanto, de acuerdo con la legislación aplicable, la Directora de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: IMPONER a ***B.B.B.*** (***Clínica de Fisioterapia Santa Fe***), con NIF ******NIF.2***, por una infracción del artículo 13 del RGPD, tipificada en el artículo 83.5 del RGPD, una sanción de apercibimiento prevista en el artículo 58.2.b) del Reglamento (UE) 2016/679.

/

SEGUNDO: IMPONER a ***B.B.B.*** (***Clínica de Fisioterapia Santa Fe***), con NIF ******NIF.2***, por una infracción del artículo 32 del RGPD, tipificada en el artículo 83.4 del RGPD, una sanción de apercibimiento prevista en el artículo 58.2.b) del Reglamento (UE) 2016/679.

Conforme al artículo 58.2.d) del RGPD, ordenar a ***B.B.B.***(***Clínica de Fisioterapia Santa Fe***), con NIF ******NIF.2***, que adopte las medidas técnicas y organizativas que sean necesarias para garantizar un nivel de seguridad adecuado al riesgo que entraña el tratamiento de datos que realiza según el artículo 32 del RGPD.

La adopción de estas medidas deberá acreditarse ante esta Agencia en el plazo de un mes computado desde la fecha en la que la resolución sea ejecutiva

TERCERO: NOTIFICAR la presente resolución a la reclamada.

CUARTO: Advertir a la sancionada que deberá cumplir la sanción impuesta una vez que la presente resolución sea ejecutiva, de conformidad con lo dispuesto en el art. 98.1.b) de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante LPACAP)

De conformidad con lo establecido en el artículo 50 de la LOPDPGDD, 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 artículo 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la LPCAP, 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.

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