938-0419
Procedimiento Nº: PS/00132/2019

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

En el procedimiento sancionador PS/00132/2019, instruido por la Agencia Española de Protección de Datos, ante la entidad CLINICAS VIVANTA SL con NIF B82809492, (en adelante "la entidad reclamada"), en virtud de la brecha de seguridad notificada a esta Agencia, con fecha 20/11/18, y teniendo como base los siguientes:

ANTECEDENTES

PRIMERO: Con fecha de 20/11/18, CLINICAS VIVANTA S.L, notifica a esta Agencia una brecha de Seguridad en la que informan de que: "*Con fecha 15/11/18, desaparece un PENDRIVE con imágenes de la cara de pacientes para tratamientos y estudios odontológicos. Entre los pacientes cuyas imágenes se encontraban grabadas había menores. Había una persona responsable de poner y quitar el dispositivo de memoria, también era responsable de su custodia*. *Cuando no se utilizaba se encontraba guardado en un cajón de un despacho con acceso restringido"*.

Han denunciado los hechos ante la Policía Nacional, (aportan copia de la denuncia) y han remitido un comunicado a todos los empleados con las prohibiciones de uso de dispositivos portátiles y la responsabilidad civil derivada de ello. Han revisado los registros de accesos con el fin de conocer la última persona que lo utilizó. Han recuperado las imágenes que existían en un ordenador de la clínica y han instalado un programa de gestión de imágenes que se utiliza en ortodoncia.

Aportan un Informe de la brecha de seguridad, de fecha 19/11/18, en el que se pone de manifiesto que: *"El día 16, la responsable del PENDRIVE donde se guardaban las imágenes de la cámara de fotos que se hacían a los pacientes de la clínica, comunica a la Directora del Centro que ha desaparecido y piensa que alguien se lo ha llevado. El dispositivo no tenía clave de seguridad para acceder por lo que lo consideran una posible brecha de seguridad. Los datos contenidos en el dispositivo eran además de las imágenes el nombre y apellido de los pacientes. Las consecuencias podrían ser una posible divulgación de la información*".

SEGUNDO: A la vista de los hechos expuestos en los documentos aportados, la Subdirección General de Inspección de Datos procedió a realizar actuaciones para su esclarecimiento de los hechos, al amparo de los poderes de investigación otorgados a las autoridades de control en el art. 57.1 del RGPD y así, el 28/01/19, se dirige requerimiento informativo a la entidad CLINICAS VIVANTA SL., solicitando, entre otras, información sobre las causas que han hecho posible la incidencia.

TERCERO: Con fecha 15/02/19, la entidad CLINICAS VIVANTA S.L, aporta la siguiente información: "*No se ha localizado el PENDRIVE que desapareció, por lo que no disponen de nueva información sobre la brecha notificada ni con respecto a la denuncia policial. Además de las medidas que se han detallado en la comunicación de la brecha de seguridad, con fecha 24/11/18 remitieron a todas las Clínicas por correo electrónico corporativo, la Política de Seguridad de la empresa. No tienen conocimiento de la utilización por terceros de los datos obtenidos a través del robo. Las imágenes tomadas para tratamiento de ortodoncia que son realizados en la*

clínica, por lo que, la imagen tomada no es completa, y no es información suficiente para realizar actividades de suplantación de identidad. No han notificado la incidencia a los afectados, ya que sus tratamientos de ortodoncia no se han visto afectados.

Aportan copia de la evaluación de impacto realizada en relación con este tratamiento de datos "Fotografías para tratamiento dental" en el que se determina que*: "Se ha evaluado la probabilidad de impacto de 56 amenazas, siendo el resultado del análisis de riesgos de este tratamiento ponderado como ACEPTABLE; Se deben implementar políticas de cifrado de datos y de disociación de datos personales y una vez implantadas las medidas, será necesaria la revisión y comprobación de su eficacia".*

CUARTO: Con fecha 10/04/19, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la entidad reclamada, en virtud de los poderes establecidos en el artículo 58.2 del RGPD y en los artículos 47, 64.2 y 68.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD), por la infracción del artículo 32.1 del RGPD tipificada en el artículo 83.4.a) del RGPD y considerada grave, a efectos de prescripción, en el 73.f) de la LOPDGDD.

Se indica además que, a los efectos previstos en el art. 64.2 b) de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, la sanción que pudiera corresponder sería de APERCIBIMIENTO, sin perjuicio de lo que resulte de la instrucción posterior.

QUINTO: Notificado el acuerdo de inicio, la entidad CLINICAS VIVANTA SL., mediante escrito de fecha 29/04/19, formuló, en síntesis, las siguientes alegaciones:

"(…) CLÍNICAS VIVANTA realizó la notificación de brecha de seguridad. La información que en su día de facilitó se realizó en el entendimiento de que la pretensión de la normativa con esta medida de notificación, es garantizar la privacidad y los derechos de los potenciales afectados, a fin de conocerse el alcance que puede llegar a tener y, poder llevar a cabo las actuaciones que se consideren oportunas, y no como un pretexto que permita abrir un procedimiento sancionador.

No obstante, esta actuación puede ser contraría a la buena fe, toda vez que, una vez se ha tenido constancia de la totalidad de la información afectada, que además fue comunicada a la AEPD a raíz de la solicitud de ampliación de información sobre la brecha de seguridad, la cual fue contestada en tiempo y forma por esta parte, los hechos no darían lugar a la comunicación de una brecha de seguridad en los términos establecidos por la AEPD en su guía informativa sobre las mismas, dado que el número total de afectados no supera el número de 20 personas, las imágenes que estaban contenidas en el pen drive, no reflejaban la totalidad de la imagen de los pacientes, y no se ha tenido hasta la fecha constancia de reclamación/denuncia por parte de ninguno de los sujetos cuyas imágenes contenía el pen drive.

La AEPD en su guía de brechas de seguridad, indicada en concreto que "con relación a las posibles sanciones que pudieran derivar de las mismas, decir que la notificación no implicará de forma directa la imposición de una sanción por parte de la AEPD, ésta sería el resultado de falta de medidas de diligencia de responsables y encargados cuando suponga la falta de medidas de seguridad adecuadas de los tratamientos y se produzca un posible perjuicio para los derechos y deberes de los interesados".

La entidad considera que sí ha tomada las medidas de diligencia suficientes, y en ningún momento la incidencia se ha producido por una falta total de medidas de

seguridad, ya que el pen drive perdido, se ubicaba en un cajón con llave, con acceso restringido sólo a una persona que contaba con la autorización para su uso y manejo, e insistimos nuevamente, no se ha tenido conocimiento de perjuicio para los derechos y deberes de los interesados que se han podido ver afectados por la incidencia, ya que no se ha tenido constancia de reclamación alguna, y ninguno de ellos se ha visto afectado en la continuidad de la asistencia sanitaria que hasta la fecha se les ha venido prestando.

Por tanto, se estaría penalizando a CLÍNICAS VIVANTA por un "exceso de diligencia", algo que parece totalmente contrario al espíritu de la normativa.

Así mismo, en cuanto a la constante indicación de la falta de medidas de seguridad, que la AEPD marca en su escrito, CLÍNICAS VIVANTA, una vez conocida el alcance de la incidencia, y así ha sido notificado tanto en la primera comunicación de 22 de noviembre de 2018, como en la segunda de fecha 15 de febrero de 2019, ha establecido un protocolo interno de respuesta a este tipo de situaciones, que incluye: la Presentación de denuncia a la Policía a fin de dejar constancia de la pérdida del pen drive; la comunicación a todos los usuarios sobre las obligaciones en materia de seguridad y específicamente sobre el uso de memorias portátiles, que es adecuado para la correcta protección de los datos y que ha sido infringido por parte del usuario que ha perdido la información y, por lo que fue debidamente sancionado por parte de CLINICAS VIVANTA y complementariamente, se han llevado a cabo medidas complementarias para evitar que pueda volver a producirse una contingencia de este tipo.

Por tanto, se ha acreditado en cumplimiento del deber de diligencia antes de la incidencia, durante la misma (comunicación preventiva de los hechos a las tanto a la Policía como a la AEPD) y después de la mismas (adopción de medidas disciplinarias contra los responsables y refuerzo de las medidas de seguridad adoptadas).

Como esta parte ha señalado dentro del presente escrito, hasta la fecha no se ha tenido conocimiento ni constancia de reclamación alguna por parte de alguno de los afectados cuya información se ha podido ver afectada por la incidencia aquí controvertida.

La prestación que hasta la fecha ha venido desempeñando sobre los sujetos afectados, no se ha interrumpido en ningún momento, ni se ha tenido que retrasar en caso alguno, por lo que no se ha producido una afectación en los derechos y deberes fundamentales de dichos sujetos, no produciéndose por lo tanto uno de los factores que en palabras de la propia AEPD en su guía de brechas de seguridad, son precisos para la iniciación de un procedimiento sancionador derivado de la notificación de una brecha de seguridad.

En cualquier caso, el número total de afectados por la incidencia es muy reducido, no superando el número de 20 sujetos interesados, y en todo caso, las consecuencias conocidas de afectación a su privacidad, como ya hemos señalado, o bien no existen, o bien no han sido comunicados a esta parte hasta la fecha.

La información que se ha visto afectada por la incidencia, se trata de fotografías de las bocas de los pacientes que estaban siendo sometidos a proceso de ortodoncia, es decir, imágenes parciales de la boca de los pacientes que eran utilizados con la única finalidad de conocer la evolución del tratamiento, por lo que el uso que se puede derivar de las imágenes por parte de un tercero no autorizado, no puede dar lugar a consecuencias sobre los derechos y libertado de los interesados afectados.

SEXTO: Con fecha 15/03/19, se inició el período de práctica de pruebas, acordándose: a).- dar por reproducidos a efectos probatorios la documentación facilitada por la Unidad de Estudios Tecnológicos sobre la comunicación de la brecha de seguridad, los documentos obtenidos y generados que forman parte del expediente E/10485/2018 y b).- dar por reproducido a efectos probatorios, las alegaciones al acuerdo de inicio del PS/132/2019, presentadas por la entidad denunciada.

SÉPTIMO: Con fecha 29/05/19, se notifica la propuesta de resolución sancionadora consistente en que por parte de la Directora de la Agencia Española de Protección de Datos se proceda al archivo del presente procedimiento sancionador al no existir vulneración de lo estipulado en el RGPD.

OCTAVO: Notificada la propuesta de resolución, la entidad no presenta ningún tipo de alegaciones a la misma, en el periodo concedido al efecto.

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

1º Con fecha de 20/11/18, CLINICAS VIVANTA S.L, notifica a la esta Agencia una brecha de Seguridad en la que informan de que, el día quince del mismo mes, ha desaparecido un pendrive, de una de sus clínicas, con imágenes del tratamiento bucodental de una veintena de pacientes.

2º Con fecha 15/02/19, la entidad indica que, aún no se ha localizado el pendrive. No obstante, se remitieron a todas las clínicas por correo electrónico corporativo, la Política de Seguridad de la empresa. Tampoco tienen conocimiento de la utilización por terceros de los datos obtenidos a través del robo. No han notificado la incidencia a los afectados, ya que sus tratamientos de ortodoncia no se han visto afectados.

3º La entidad aportan copia de la evaluación de impacto realizada en relación con este tratamiento de datos, en el que se determina, entre otras, que: *"Se ha evaluado la probabilidad de impacto de 56 amenazas, siendo el resultado del análisis de riesgos de este tratamiento ponderado como ACEPTABLE; Se deben implementar políticas de cifrado de datos y de disociación de datos personales y una vez implantadas las medidas, será necesaria la revisión y comprobación de su eficacia*".

4º En el escrito de fecha 29/04/19, la entidad indica que ha establecido un protocolo interno de respuesta a este tipo de situaciones, que incluye: *"la presentación de denuncia a la Policía. La comunicación a todos los usuarios sobre las obligaciones en materia de seguridad y específicamente sobre el uso de memorias portátiles, que es adecuado para la correcta protección de los datos para evitar que pueda volver a producirse una contingencia de este tipo.*

5º Hasta la fecha no se ha tenido conocimiento ni constancia del alguna por parte de alguno de los afectados cuya información se ha podido ver afectada por la incidencia aquí controvertida.

FUNDAMENTOS DE DERECHO

I

En virtud de los poderes que el artículo 58.2 del RGPD reconoce a cada autoridad de control, y según lo establecido en el art. 47 de LOPDGDD, la Directora de la Agencia Española de Protección de Datos es competente para resolver este procedimiento.

II

Los apartados 1) y 2), del artículo 58 el RGPD, enumeran, respectivamente, los poderes de investigación y correctivos que la autoridad de control puede disponer al efecto, mencionando en el punto 1.d), el de: "*notificar al responsable o encargo del tratamiento las presuntas infracciones del presente Reglamento"* y en el 2.i), el de: "*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.".*

La valoración conjunta de la prueba documental obrante en el procedimiento trae a conocimiento de la AEPD una visión de la actuación de la entidad reclamada, que ha quedado reflejada en los hechos declarados probados.

En el presente caso, la entidad ha declarado la evaluación de impacto, en relación con el riesgo en el tratamiento de datos personales, como aceptable ya que las imágenes tomadas para el tratamiento de ortodoncia no son completas, no siendo información suficiente para realizar actividades de suplantación de identidad. También indica que ha establecido un protocolo interno de respuesta ante este tipo de situaciones como son, denuncia ante la Policía Nacional, indicaciones a los empleados sobre las prohibiciones de uso de dispositivos portátiles y la responsabilidad civil derivada de ello, revisión de los registros de accesos a los dispositivos y la instalación de un programa de gestión de imágenes que incluirá de cifrado y disociación de datos personales.

Por lo tanto, de la información aportada por la entidad a esta Agencia, tanto en la inspección previa como en las alegaciones a la incoación del expediente, se desprende que las posibles deficiencias en materia de medidas de seguridad han sido subsanadas para evitar un nuevo problema, y, de esta forma, cumplir lo estipulado en el artículo 32.1 del RGPD, en relación con el tratamiento de los datos y las medidas técnicas y organizativas necesarias para garantizar un nivel de seguridad aceptable.

Vistos los preceptos citados y demás de general aplicación, la Directora de la Agencia Española de Protección de Datos RESUELVE**:**

PRIMERO: ARCHIVAR el presente procedimiento sancionador contra la entidad CLINICAS VIVANTA SL, por una supuesta infracción del artículo 32.1) del RGPD.

SEGUNDO: NOTIFICAR la presente resolución a la entidad CLINICAS VIVANTA SL.

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 art. 48.6 de la LOPDPGDD, 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.

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