Expediente Nº: EXP202307460

RESOLUCIÓN DE TERMINACIÓN DEL PROCEDIMIENTO POR PAGO VOLUNTARIO

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

ANTECEDENTES

PRIMERO: Con fecha 17 de abril de 2024, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a **DENTALCUADROS BCN S.L.P.** (en adelante, la parte reclamada), mediante el Acuerdo que se transcribe:

<<

Expediente N.º: EXP202307460

ACUERDO DE INICIO DE PROCEDIMIENTO SANCIONADOR

De las actuaciones practicadas por la Agencia Española de Protección de Datos y en base a los siguientes

HECHOS

PRIMERO: Con fecha 12 de mayo de 2023, se notificó a la División de Innovación Tecnológica de esta Agencia una brecha de datos personales remitida por DENTALCUADROS BCN S.L.P. con NIF B67480376 (en adelante, DENTALCUADROS) como responsable del tratamiento, relativa a un ciberincidente de tipo Ransomware que afectó a la disponibilidad y confidencialidad de datos personales.

En la notificación de la brecha de datos personales se aporta la siguiente información:

- Descripción incidente: "*Detección de un Malware en el ordenador servidor de la empresa. Imposibilidad de acceder al sistema informático utilizado para recopilación de datos de pacientes. Todos los datos fueron encriptados y se encontró un correo electrónico solicitando un rescate económico para recuperar dichos datos*."

- Fecha de detección de la brecha: 20 abril 2023.

- Categoría de datos afectados: básicos (Ej: nombre, apellidos, fecha de nacimiento), DNI, NIE, Pasaporte y / o cualquier otro documento identificativo, Datos económicos o financieros (sin medios de pago), Datos de contacto, De salud.

- Número de afectados: 2500 pacientes.

- Se afirma que los afectados serán informados.

- Se afirma que se ha interpuesto denuncia ante autoridades policiales.

SEGUNDO: Como consecuencia de los hechos conocidos, con fecha 30 de mayo de 2023 la Directora de la Agencia Española de Protección de Datos ordenó a la Subdirección General de Inspección de Datos (SGID) realizar las oportunas investigaciones previas con el fin de determinar una posible vulneración de la normativa de protección de datos.

TERCERO: 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:

En fecha 2 de agosto de 2023 se realiza un primer requerimiento de información dirigido al responsable de tratamiento DENTALCUADROS marcado por la siguiente línea de investigación:

- Solicitar e investigar el registro documentado de la brecha de seguridad.
- Investigar el Registro de Actividades de Tratamiento para la actividad afectada por la brecha.
- Investigar tanto la comunicación a los afectados como el motivo del retraso en la notificación de la brecha.
- Investigar los análisis de riesgos existentes para los derechos y libertades de las actividades de tratamiento afectadas así como la posible Evaluación de Impacto.
- Investigar las medidas preventivas que existían y las reactivas implantadas tras la brecha.
- Solicitar copia de la denuncia interpuesta.

En fecha 2 de agosto de 2023 consta acuse de recibo por parte de DENTALCUADROS al requerimiento anterior, notificado por vía electrónica, en el que se concedió el plazo de 10 días para contestar; no obstante, a fecha 31 de agosto de 2023 y habiendo finalizado dicho plazo, no se había recibido respuesta, decidiéndose reiterar la notificación del requerimiento anterior en esa misma fecha, 31 de agosto de 2023.

En fecha 9 de octubre de 2023, y tras no recibirse respuesta a la reiteración del requerimiento, se decide por parte del inspector contactar vía email con el Delegado de Protección de Datos del investigado, poniendo en su conocimiento los dos requerimientos notificados y no respondidos, informando de la obligación de facilitar los documentos, informaciones y cualquier otra colaboración que se precise en las actuaciones de inspección.

En fecha 10 de octubre de 2023 se recibe respuesta del Delegado de Protección de Datos con el siguiente texto:

(…).

En fecha 10 de octubre de 2023 se constata la recepción de la respuesta a la reiteración del requerimiento, de su análisis se extrae las siguientes afirmaciones relevantes para la investigación:

- El día 20 de abril de 2023 tuvieron problemas al intentar entrar en el sistema informático y acceder a los datos de pacientes, localizando un fichero que contenía un mensaje en el que se solicitaba rescate por los datos encriptados.

- Puesto que, el disco duro estaba encriptado, procedieron a sustituirlo en fecha 24 de abril de 2023, reinstalando el software necesario.

- La última copia de seguridad que disponían tenía una antigüedad de un mes aproximadamente y estaba guardada en un disco duro externo, esta copia sirvió para recuperar todos los datos de pacientes hasta esa fecha. Afirman lo siguiente: "*A partir de ahí se pudo comenzar a trabajar con normalidad, aunque con el inconveniente principal de haber perdido la agenda de citas de los pacientes…Los datos que se perdieron del último mes se han podido ir recuperando con normalidad, las citas con los pacientes han permitido recuperar la información de los tratamientos que se les habían realizado y darles continuidad*".
- En relación con el ordenador afectado afirman que: "*El ordenador servidor disponía de antivirus, pero la brecha se produjo a través de un puerto abierto para conexión remota, y no fue suficiente*".
- El ordenador disponía de antivirus, pero la brecha se produjo a través de un puerto abierto para conexión remota.
- Afirman que tras la brecha decidieron ***(…)***.
- El número de afectados aproximado es de 2500, todos ellos pacientes, con datos identificativos, de salud y económicos sobre pagos, pero sin existir números de cuenta bancaria o números de tarjetas de crédito.
- Afirman que no han recibido comunicación o quejas de pacientes alertando de la materialización de posibles consecuencias y que han monitorizado internet sin obtener exposición de datos.
- Se adjunta un informe del incidente redactado por la empresa informática que da soporte técnico a DENTALCUADROS, de su análisis se extrae:
    - El informe está redactado por la empresa JOSEP MOLINS SERVEIS INFORMATICS.
    - En el informe se afirma que la noche del 20 al 21 de abril de 2023 "*hackers consiguen entrar por la brecha del puerto 3389 abierto en el router para la conexión de escritorio remoto, procediendo a encriptar todos los ficheros de datos incluido Microsoft SQL…Cabe destacar que como el ataque se produce de madrugada, el resto de los ordenadores de la clínica están apagados con lo que no consiguen encriptar*".
    - Se afirma

> "*Como ya se sabe que pretenden extorsionar económicamente y rechazándolo completamente se procede a buscar copias externas de los datos encriptados. Localizamos un disco externo donde se encuentre una copia de hace dos meses aproximadamente. Decidimos actuar con dicha copia*."
>
> "*No tenemos constancia de que los datos hayan sido robados, sino que han sido encriptados para pedir un rescate. En cualquier caso, en el programa de gestión hay fichas de pacientes y tratamientos dentales. No se guardan datos económicos como tarjetas de crédito, etc…así que la exposición solo afectaría a direcciones, teléfonos o direcciones de correo.*"

  - Se afirma que procedieron de la siguiente forma: ***(…).***

- Se adjunta el Registro de Actividades de Tratamiento (RAT) con la información de la actividad afectada por la brecha (*"Gestión de Pacientes"*), de su análisis se extrae:
  - Incluye los datos del Delegado de Protección de Datos, la empresa *SRCL Consenur SLU*.
  - Finalidad del tratamiento: *diagnosis, tratamiento e historial médico, gestión administrativa, contable y fiscal.*
  - Interesados: *pacientes, padres o tutores, representante legal.*
  - Datos: *DNI, nombre y apellidos, dirección, teléfono, firma, imagen, salud, datos biométricos, datos sobre categorías personales, datos económicos, financieros y seguros.*
  - Transferencias: *al prestador Align Technology Inc en EEUU a través de Normas Corporativas Vinvulantes.*
  - Plazos de conservación: *Historial clínico (Ley 41/2002) obliga a conservar historias clínicas un mínimo de 5 años. La Ley 21/2000 de Cataluña obliga a conservación durante 15 años de determinada información relacionada con la historia clínica.*
  - Descripción general de medidas de seguridad:
    - ***(…).***
  - Base jurídica: *prestación de servicio contratado y cumplimiento de obligación legal.*
- Afirman que el mantenimiento del servidor afectado está a cargo de la empresa INFORMED SOFTWARE, S.L (proveedora del software "*Gesden*" para la gestión de los pacientes de la clínica), aportando copia del contrato de encargo de tratamiento. Este contrato tiene fecha de firma 16 de septiembre de 2019.
- En relación con la comunicación a las personas afectadas afirman que *"se realizó de manera verbal dentro de la clínica y en las citas programadas que tenía cada paciente, informando sobre la violación sufrida y pérdida de datos del último mes debido a que la última copia no era reciente*". Afirman que no se remitió comunicación individual a cada afectado debido a que consideraron que las consecuencias tenían baja severidad para los afectados; ya que, no constaba que hubiesen utilizado los datos encriptados con fines maliciosos. Afirman que no tienen conocimiento de que se haya podido filtrar los datos, y que ningún paciente había comunicado incidencia.
- Se adjuntan cuatro documentos que contienen distintas Evaluaciones de Impacto relativa a la protección de datos (EIPD) de la actividad de tratamiento

afectada, realizadas en distintas fechas: un primer documento que contiene la evaluación inicial realizada en el año 2019, y tres documentos adicionales que contienen distintas actualizaciones de la evaluación inicial, realizadas en los años posteriores 2020, 2021 Y 2022.

- Del análisis de la primera EIPD, realizada en fecha 19 de diciembre de 2019, se extrae:
    - Se realiza una descripción del ciclo de vida de los datos, detallándose las etapas del tratamiento “captura”, “clasificación y almacenamiento”, “uso y tratamiento”, “cesión a tercero”, “destrucción”.
    - Se describen los roles que intervienen en el tratamiento, el tipo de datos al que se accede y la legitimación de este acceso.
    - Se describen los sistemas de información que intervienen en los tratamientos.
    - Se realiza análisis de necesidad y proporcionalidad del tratamiento.
    - Se analizan y evalúan los riesgos derivados de las siguientes amenazas identificadas***:***
        - ***(…).*** (A este riesgo se le asigna un valor de impacto “MÁXIMO” y probabilidad “DESPRECIABLE”, concluyendo un valor de nivel de riesgo *inherente* “MEDIO”).
        - ***(…).***
        - ***(…).*** (A este factor de riesgo se le asigna un valor de impacto “DESPRECIABLE” y una probabilidad “DESPRECIABLE”, concluyendo un valor del nivel de riesgo *inherente* “BAJO”).
        - ***(…).***
    - Se destacan los siguientes riesgos relevantes:
        - ***(…).***
    - Se incluye un plan de acción que recoge un listado de medidas a implantar para la mitigación de los riesgos, todas estas medidas tienen asignada una fecha como plazo máximo de implantación, y se afirma: “*De acuerdo con el plan de acción y en base a las amenazas detectadas, se proponen las siguientes medidas correctoras que deben implantarse en la organización antes de la fecha indicada en el plazo*”. Del listado de medidas destacan:
- ***(…).***
- Del análisis del documento que contiene la segunda EIPD realizada en fecha 15 de septiembre de 2020, se extrae:
    - Tiene idéntica estructura y contiene información similar (actualizada) a la EIPD realizada en diciembre de 2019 y analizada en punto anterior, se han modificado algunos valores para los riesgos inherentes concluidos y se ha establecido un nuevo plazo para la implantación de medidas incluidas en el plan de acción, que son las mismas que las incluidas en la EIPD de 2019.
    - Las amenazas analizadas en esta EIPD son las mismas que las analizadas en la EIPD de 2019.
    - Ha disminuido el valor asignado al nivel de riesgo “*deficiencia en la protección de la integridad*”, pasando a tener un valor de “*RIESGO BAJO*”, al haber cambiado la probabilidad de ocurrencia de “*MÁXIMA*” a “*DESPRECIABLE*”, no necesitando por tanto la inclusión de medidas adicionales en el plan de acción para adecuar este nivel de riesgo.

- El plan de acción contiene el mismo listado de medidas de seguridad concluidas en la EIPD de 2019, pero en este nuevo documento se ha asignado una nueva fecha como plazo máximo de implantación, 15 de junio de 2021 para las medidas que antes tenían como plazo máximo 19 de septiembre de 2020, y 15 de marzo de 2021 para las medidas con plazo previo 19 de julio de 2020. De esta información se concluye que las medidas no fueron implementadas tras la primera Evaluación de Impacto.

- Del análisis del documento con la tercera EIPD realizada en fecha 15 de julio de 2021, se extrae:
  - Tiene misma estructura y contenido que las anteriores, de su texto no se aprecian diferencias en relación con los riesgos identificados y evaluados, así como tampoco en la relación de medidas incluidas en el plan de acción, únicamente se detecta que se vuelve a cambiar y asignar una nueva fecha máxima de implantación.
- Del análisis del documento con la última EIDP, realizada en fecha 18 de octubre de 2022, se extrae:
  - Tiene similar estructura e información que la última EIPD. El plan de acción incluido contiene idénticas medidas a las aportadas en las evaluaciones anteriores, no obstante, se ha vuelto a cambiar y asignar nuevos plazos máximo de implantación, pasando a tener las nuevas fechas 15 de abril de 2022 y 15 de enero de 2022.
- En respuesta a la solitud para acrediten documentalmente las medidas preventivas implantadas afirman: ***(…)***.
- Se acredita documentalmente la existencia de un procedimiento para dar respuesta a las brechas de datos personales, este documento lo trasladó SRCL CONSENUR a DENTALCUADROS cuando se contrató los servicios de protección de datos (01 de noviembre de 2019). El procedimiento incorpora los textos:

  "*Cualquier usuario de DENTALCUADROS deberá notificar al responsable del tratamiento cualquier incidencia o variación que se produzca respecto de la operativa habitual. Cuando el responsable tenga conocimiento informará al DPO (si dispone de él), siendo el Responsable de tratamiento quien debe asegurarse de que se realice la notificación de la quiebra de seguridad a la Autoridad de Control."*

  "*El Responsable de tratamiento recibirá las notificaciones y las comunicará al Delegado de Protección de Datos a través de la notificación nº 17 'Notificación de Quiebras de Seguridad' en un plazo no superior a 24 horas, así como a los técnicos encargados de la seguridad del sistema."*

  "*El responsable documentará las acciones y efectos que se deriven una vez finalizada la subsanación. "*

  "*El responsable debe asegurarse que se informa de la incidencia a todos los afectados."*
- Se acredita documentalmente la existencia de un procedimiento de copias de respaldo y recuperación, redactado en el año 2020, de su análisis se extrae:

"Deberán establecerse procedimientos para la realización como mínimo semanal de copias de respaldo, salvo que en dicho periodo no se hubiera producido actualización de los datos."

"Conviene realizar una copia diaria de los datos para poder realizar una recuperación total ante pérdidas de información."

"Las copias nunca se deben guardar en lugares expuestos al público o de fácil acceso."

"Como medida para el tratamiento de datos de categorías especiales, deberá conservarse una copia de respaldo de los datos en un lugar diferente de aquél en que se encuentren los equipos que los tratan."

- Se acredita documentalmente la existencia de un procedimiento para la identificación y autenticación de los usuarios creado en el año 2020.
- En relación con las medidas reactivas adoptadas tras el incidente afirman: ***(…).***
- Se adjunta el informe sobre la brecha de seguridad redactado por el Delegado de Protección de Datos (la empresa SRCL CONSENUR S.L) y entregado al responsable de tratamiento en fecha 21 de septiembre de 2023.

De su análisis se extrae:

o Se afirma: "*Con fecha 3 de mayo de 2023 recibimos notificación de la Clínica indicándonos que con fecha 20 de abril de 2023 habían sufrido un ataque informático a consecuencia del cual se habían visto comprometidos datos personales"*. Se aporta captura de pantalla con el correo electrónico que acredita esta notificación, enviado desde la dirección ******EMAIL.1*** y con el siguiente contenido:

> ***"****Escribo para informar de que el día 20/04/2023 la clínica DentalCuadros BCN, SLP ha sufrido un ataque informático, encriptando toda la información que se encontraba en el servidor y el programa informático que se utiliza para tratar datos y tratamientos de pacientes. La última copia de seguridad que había era del 14/03/2023 pudiendo recuperar los datos hasta esa fecha*.
> *Se ha hecho denuncia ante los Mossos y desde el COEC nos han dicho que debemos informaros de esta situación*. *Necesitan algún dato más? Se encargan de informar a la Agencia Española de Protección de Datos?*"

o Se afirma que, tras recibir la comunicación anterior, el DPD mantuvo contacto telefónico con el responsable DENTALCUADROS para recabar más información, remitiéndole un formulario modelo de notificación para que incluyeran en él todos los detalles del incidente y se lo remitieran cumplimentado. Afirman que hasta el día 9 de mayo no reciben la respuesta de DENTALCUADROS con el formulario cumplimentado, y que en esta misma fecha el DPD procede a realizar una valoración del incidente para poder proporcionar indicaciones al responsable sobre la necesidad y obligatoriedad de la notificación tanto a la AEPD como a los afectados. En relación con esto se extraen las afirmaciones:

"*Teniendo en cuenta la naturaleza del ataque, el elevado número de personas afectadas así como el alto volumen de datos afectados, y el carácter especialmente sensible de algunos de ellos, y las consecuencias que este podría acarrear para los derechos y libertades de los afectados, como puede ser la divulgación de datos personales, la usurpación de identidad, la imposibilidad de ejercicio de derechos, la no continuidad de prestación sanitaria, la pérdida de confidencialidad de datos afectados por secreto profesional, desde SRCL CONSENUR, se traslada al responsable de tratamiento el día 10 de mayo de 2023 la necesidad de comunicar el incidente sufrido , lo antes posible, ante la Agencia Española de Protección de Datos y también a los pacientes afectados*".

"El día 12 de mayo de 2023 nuestro cliente realiza la notificación a la AEPD de la brecha de seguridad, y desde SRCL CONSENUR procedemos a elaborar una carta informativa para que el responsable de tratamiento pueda personalizar y enviar a los pacientes afectados por la brecha"

"El día 24 de mayo de 2023, y debido a que el servicio informático en esa fecha sigue sin poder confirmar si el ataque ha ocasionado el acceso no autorizado a los datos personales o únicamente el cifrado de la información, se envía a la clínica el modelo de carta informativa para que puedan personalizarlo y hacérselo llegar a todos los pacientes afectados a los cuales tengan opción de localizar a través de correo postal o correo electrónico, y además, debido a que según nos indica la clínica hay un número de pacientes a los que no se les puede localizar al haber sido atendidos por primera vez entre el 14 de marzo de 2023 y el 20 de abril de 2023, fechas en las que no se cuenta con copias de seguridad, se indica que pueden poner aviso informativo, ya sea colocando un cartel en la entrada de la clínica que pueda leerse si se pasase por delante o a través de medios digitales, para que los pacientes atendidos por primera vez entre esas fechas acudan a la clínica para que se les informe del incidente sufrido"

- Se aportan también las siguientes afirmaciones relevantes*:*

"Durante el proceso de valoración del incidente, en varias ocasiones se contacta con el cliente con el fin de informarle en relación a la necesidad de disponer de un exhaustivo informe por parte de su servicio informático…con la finalidad de determinar si la brecha producida se correspondía con una brecha de integridad, disponibilidad, confidencialidad o cualquier combinación, y al no obtenerse mayor información, debemos catalogarlo como una brecha de confidencialidad y disponibilidad. De confidencialidad sobre el total de los datos personales al no poder confirmar si el atacante accedió a los datos personales; y de disponibilidad sobre los datos personales de los que no se disponía copia de seguridad (para todos los datos personales recogidos desde el 14 de marzo de 2023 hasta el día del ataque)."

"Además de las medidas propuestas por el cliente, se recomienda por parte de SRCL CONSENUR:

-La revisión por parte de la clínica de la correcta implantación de las medidas recogidas en la última EIPD y en la auditoría realizadas.

-La realización por parte de su servicio informático de una revisión/auditoría de los sistemas afectados.

-La importancia de poner a disposición del personal con acceso a datos personales de los procedimientos incluidos en el documento de seguridad.

-La notificación del incidente a los afectados por la brecha."

"Con fecha 13 de septiembre de 2023 recibimos comunicación por parte de la clínica en la que nos informan de la recepción de un requerimiento de información adicional por parte de la AEPD. En conversación telefónica del día 14 de septiembre de 2023 con la persona de la clínica encargada de gestionar este asunto, nos trasladan la recepción de un segundo requerimiento sobre la brecha y nos manifiestan el desconocimiento del día exacto en el que recepcionan/abren la notificación que remite la AEPD con fecha 31 de agosto de 2023. En este momento se la hacen las indicaciones al cliente para dar respuesta a todos y cada uno de los puntos que solicita la AEPD, en tiempo y forma."

Asimismo, nos indican que, por una decisión interna de la Clínica, no se notificó a los pacientes a través de la carta si no que se realizó verbalmente a un número determinado de pacientes."

- En respuesta a la solicitud de que expliquen el motivo de la dilación temporal en la notificación de la brecha, el responsable afirma:

"*Fueron días de intentar recuperar datos de pacientes para poder seguir trabajando e intentar entender lo que sucedía, por ello la siguiente medida fue presentar la denuncia ante autoridades policiales ya que no sabíamos el alcance de la situación. Es por ello por lo que no sabíamos la necesidad de informar a la AEPD, ya que disponíamos de muy poca información y estábamos pendientes de recopilar datos, siendo esta la primera vez que nos ocurre algo así"*.

- Se aporta copia de la denuncia presentada ante las autoridades policiales, de su análisis no se extrae información adicional a la ya aportada en puntos anteriores. No obstante, en la denuncia se visualizan varias capturas de pantallas adjuntas donde se muestra el mensaje que dejaron los atacantes con un fichero en el servidor.
- En relación con las medidas para garantizar la disponibilidad de la información se afirma en la respuesta al requerimiento: ***(…)***.
- En relación con las medidas para garantizar la formación y concienciación de los empleados en materia de seguridad y tratamiento de datos personales se afirma: ***(…)***.

En fecha 18 de octubre de 2023 se realiza nuevo requerimiento marcado por la siguiente línea de investigación:

- Que confirmen si entre los datos afectados se encontraban copias de DNI de pacientes.
- Que aclaren el tipo de datos biométricos que se necesitaban recabar en la actividad de tratamiento afectada (*Gestión de Pacientes*), según la información contenida en el RAT.
- Investigar las medidas de seguridad implantadas para garantizar los accesos por escritorio remoto a través del puerto habilitado (3389).
- Solicitar aclaración sobre el motivo por el que decidieron no atender la recomendación realizada por el DPD en relación con la necesidad de notificar a los afectados de forma directa por correo electrónico o postal.
- Solicitar la aportación de las capturas de pantalla que aparecen en la denuncia ante autoridades policiales.

En fecha 30 de octubre de 2023 se recibe respuesta al requerimiento anterior, de su análisis se extrae la siguiente información relevante para la investigación:

- Afirman:

"*En primer lugar, y antes de proceder a dar respuesta a las cuestiones que nos plantea sobre la brecha de seguridad sufrida, creemos importante, por la relevancia que tiene, trasladar las ultimas averiguaciones realizadas ya que, en nuestra opinión, cambia el alcance de la misma y las consecuencias que se derivan para nuestros pacientes. En las últimas conversaciones mantenidas con Infomed Software, S.L. (Infomed), empresa proveedora de los software de gestión (Gesden) y firma digital de documentos por los pacientes (Clinipad) donde se almacenaban la inmensa mayoría de datos afectados, nos indica que Gesden (donde se almacenan tanto la información introducida en ese programa como la información generada con Clinipad) dispone de medidas de cifrado de la información que contiene, al igual que las contraseñas de acceso, por lo que el atacante, si bien accedió al dispositivo, no puedo acceder a la información que en este programa se almacenaban. Fuera de ese programa se almacenaban, en otro software distinto y en otro disco duro las radiografías de los pacientes, sólo se pueden visualizar en Gesden cuando este disco duro está encendido, pero no se quedan guardadas. En el momento del ataque, ese disco estaba desconectado"*.

- En respuesta a nuestra pregunta para que confirmen si trataban copias digitalizadas de DNI de pacientes, afirman que únicamente trataban números de DNI.

- En respuesta a nuestra pregunta para que aclaren el tipo de datos biométricos mencionados en el RAT para la actividad "*Gestión de Pacientes*", afirman que estos datos son, por un lado, las ortopantomografías realizadas a los pacientes y, por otro lado, los datos asociados a la firma digital que realizan los pacientes a través de una Tablet para la firma de los consentimientos sanitarios, y que estos últimos se almacenaban en el software Gesden, con medidas de seguridad para la protección, por lo que el atacante no habría tenido acceso a

ellos. En el caso de las ortopantomografías, afirman que sólo eran visibles desde *Gesden* y que el disco duro que las almacena estaba desconectado.

- En respuesta a nuestra pregunta para que acrediten si existía alguna medida de seguridad para proteger el servicio de escritorio remoto, como por ejemplo la posible implantación de VPN, existencia de Firewall o reglas de limitación de acceso al puerto remoto, afirman:

"Se utilizaba como Firewall el propio de Microsoft incorporado en Windows Server. Estamos trabajando en contratar una empresa especializada y añadir más medidas de seguridad y de cifrado adicional que sean necesarias."

- En relación con nuestra solicitud para que justifiquen el motivo por el que decidieron no atender la recomendación del DPD sobre la necesidad de comunicar la brecha de forma directa a cada paciente afectado vía email o correo postal, afirman que decidieron realizar comunicación verbal a los pacientes según acudían a la clínica, aportando los siguientes motivos justificativos:

"*Desde la clínica se decidió modificar el tipo de comunicación a realizar a los pacientes debido a que, en los días posteriores al incidente y la comunicación de la brecha ante la Agencia Española de Protección de Datos, confirmamos que ningún dato financiero o económico como número de tarjeta o cuenta bancaria se vio afectado, y, por lo tanto, las posibilidades de que nuestros pacientes sufriesen un delito financiero se vieron reducidos*.

Asimismo, y aunque conscientes de la sensibilidad y de la importancia de los datos que recogemos sobre nuestros pacientes en una clínica dental, los datos de salud recogidos en una Clinica dental como la nuestra y las anotaciones realizadas en los historiales clínicos de nuestros pacientes, en muchas ocasiones son de carácter técnico, requiriéndose para su entendimiento conocimientos bastante específicos sobre odontología o medicina que dificultan el entendimiento de los mismos en caso de producirse una exposición pública de esos datos por un tercero que no posea dichos conocimientos.

Respecto al ejercicio de derechos, la clínica valoró a la hora de cambiar el tiempo de notificación, el hecho de que la gran mayoría de los pacientes que soliciten su derecho de acceso (Conforme a la normativa sanitaria o a la normativa de protección de datos) podrán ver atendido su derecho de manera positiva, al haber podido recuperar la copia de seguridad que contenía los datos personales de nuestros pacientes hasta el día 14 de marzo de 2023.

También se tuvo en cuenta desde la clínica para llevar a cabo un cambio en la forma de comunicar a los afectados la brecha de seguridad:

> *-El hecho de que no todos los pacientes facilitan su correo electrónico a la hora de recabar sus datos y en los casos en los que sí que lo han facilitado, no podemos garantizar que ese dato se encuentre actualizado, ya que los pacientes pueden haber cambiado de dirección electrónica y no haber comunicado dicho cambio a la clínica al no haber acudido al centro a realizarse algún tratamiento dental tras ese cambio de dirección.*
>
> *-El alto coste para la clínica del envío por correo postal de cartas a todos y cada uno de los pacientes dados de alta en nuestra base de datos, sin poder garantizar de ese modo que la información llegue a todos nuestros pacientes considerando, por ejemplo, probables cambios de domicilio de los pacientes de los que no seamos conscientes en la Clínica*
>
> *-En relación a los pacientes que acudieron por primera vez entre el día 14 de marzo y el día que se produjo la brecha de seguridad, al no disponer de copia de seguridad, se perdió toda la información y no disponíamos ni de su correo electrónico ni de su dirección postal para localizaros, por lo que la única opción viable es recabar nuevamente su información en la próxima visita y explicarles el incidente verbalmente en ese momento en el que acuden a la segunda visita al centro*
>
> *-La alarma o nerviosismo que se podría generar entre los pacientes al recibir la notificación de carácter genérico, que podría provocar una entrada masiva de llamadas, correos electrónicos y visitas en la clínica que perjudicarían al centro, a los pacientes que requieren atención sanitaria preferente y a las labores de recuperación de la información perdida en la que estábamos inmersos."*

- Se aportan las capturas de pantallas de poca legibilidad incluidas en la denuncia, no se aporta información adicional relevante a la ya aportada en puntos anteriores.

Dada la necesidad de aclaración de algunos puntos, en fecha 7 de noviembre de 2023 se decide llevar a cabo un último requerimiento marcado por la siguiente línea de investigación:

- Solicitar que acrediten las medidas de cifrado que según afirmaban les habían sido trasladadas en las últimas conversaciones por parte de la empresa proveedora del software *Gesden*, y de las cuales no tenían conocimiento anterior.

- Solicitar acreditación de la política de gestión de usuarios en el software *Gesden*.

- Solicitar acreditación del contrato de encargo con la empresa JOSEP MOLINS SERVEIS INFORMATICS, que daba soporte técnico a DENTALCUADROS y no había sido aportado en requerimientos anteriores.

- Solicitar detalles del tipo de datos personales almacenados en el servidor al margen de *Gesden*.

- Solicitar detalles sobre el tipo de vulnerabilidad del puerto 3389 que fue explotada por los atacantes.

- Solicitar que confirmen cuáles de las medidas incluidas en el plan de acción de la última EIPD no se habían implantado aún en la organización.

En fecha 15 de noviembre de 2023 se recibe respuesta al requerimiento anterior, de su análisis se aporta a la investigación:

- En respuesta para que acrediten las medidas de cifrado descubiertas en *Gesden* afirman: "*La base de datos del programa está almacenada en un servidor de SQL. Para acceder a ella hace falta entrar como el super administrador de SQL*".

- En relación con los usuarios y política de contraseñas de *Gesden* afirman:

"*En la empresa se establecen diferentes grupos de usuarios como el usuario administrador, profesionales (odontólogos y auxiliares) y recepcionista. Los perfiles de acceso se establecen en función de las necesidades de acceso a datos de los usuarios, siendo el usuario administrador el que posee los privilegios completos y tiene la capacidad de modificar, bloquear y eliminar usuarios, así como dar los permisos que correspondan a cada uno"*.

"*Existe política de contraseñas en el software con la opción de que la pueda configurar la propia clínica, cada usuario establece su propia contraseña, y se configuran los periodos de validez, longitud, número de intentos para acceder.*"

- Se aporta contrato de encargo de tratamiento con la empresa encargada del soporte técnico informático (*Josep Molins Serveis Informatics*), este contrato tiene fecha de firma 9 de octubre de 2019.

- En relación con nuestra consulta para que aporten información sobre la vulnerabilidad explotada a través del puerto 3389 del servidor, indicando si se trataba de Cryptolocker:

"*Han existido más de 25 vulnerabilidades del Puerto 3389 en Windows Server 2016, la más destacada es BlueKeep, esta permite la entrada de software Cryptolocker. Se utilizaba como Firewall el propio de Microsoft incorporado en Windows Server*"

- Sobre la posibilidad de que fuera la vulnerabilidad BlueKeep (publicada en mayo de 2019) se afirma:

"*Se consulta al informático y nos explica que él no pudo confirmar este dato, debido a que tras el ataque el ordenador quedó inservible, y fue por eso por lo que tuvo que cambiar el disco duro interno".*

- En respuesta a nuestra solicitud para que aporten información sobre la política de actualización del servidor responden:

"*El servidor estaba configurado para realizar actualizaciones automáticas, tal y como venía por defecto en Windows Server.*"

- En respuesta a nuestra solicitud para que acrediten y confirmen si se llevaron a cabo las medidas de formación en seguridad incluidas en el plan de acción afirman:

"*Al inicio de la relación laboral con los trabajadores se les indican pautas de seguridad a cumplir en la empresa, y se les hace entrega para su lectura y firma del documento de confidencialidad y un listado de obligaciones que contraen con la empresa. Se adjunta documento.*

Se les indica a los empleados la necesidad de realizar un curso informativo elaborado por el INCIBE, y se les facilita el enlace https://itinerarios.incibe.es/, indicándoles la importancia de la formación en materia de seguridad.

Se ha preparado un documento en la empresa con los puntos clave que consideramos que los trabajadores deben tener siempre en cuenta en sus puestos de trabajo, de una forma sencilla para que puedan estar más claras las medidas de seguridad."

- En relación con nuestra solicitud para que confirmen todas las medidas incluidas en el plan de acción de la EIPD que aún no habían sido implantadas, no se recibe información.

QUINTO: De acuerdo con el informe recogido de la herramienta AXESOR, la entidad DENTALCUADROS BCN S.L.P. es una microempresa constituida en el año 2019, y con un volumen de negocios de 517.290 euros en el año 2022.

FUNDAMENTOS DE DERECHO

I
Competencia

De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada autoridad de control y según lo establecido en los artículos 47, 48.1, 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 (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
Obligación incumplida

En el presente caso, de acuerdo con lo establecido en el artículo 4.1 del RGPD, consta la realización de un tratamiento de datos personales, toda vez que DENTALCUADROS realiza, entre otros tratamientos, la recogida, conservación, consulta, utilización, acceso de los siguientes datos personales de clientes, tales como: nombre, apellidos, fecha de nacimiento, DNI, NIE y/o Pasaporte, datos de contacto, datos económicos y datos de salud dental …, etc.

DENTALCUADROS realiza esta actividad en su condición de responsable del tratamiento, dado que es quien determina los fines y medios de tal actividad, en virtud del artículo 4.7 del RGPD.

El artículo 4 apartado 12 del RGPD define, de un modo amplio, las "*violaciones de seguridad de los datos personales"* (en adelante brecha de datos personales) como "*todas aquellas violaciones de la seguridad que ocasionen 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.*"

En el presente caso, consta una brecha de datos personales en las circunstancias arriba indicadas, categorizada como una brecha de disponibilidad por cuanto el ataque se materializó en la imposibilidad de acceder al sistema informático utilizado para la recopilación de datos de pacientes, todos los datos personales fueron encriptados, quedando acreditado que recibieron un mensaje por parte del grupo criminal Ransomware (Hive) confirmando la autoría del ataque y solicitando pago de un rescate para la recuperación de dichos datos.

Hay que señalar que la identificación de una brecha de datos personales no implica la imposición de una sanción de forma directa por esta Agencia, ya que es necesario analizar la diligencia de responsables y encargados y las medidas de seguridad aplicadas.

Dentro de los principios del tratamiento previstos en el artículo 5 del RGPD, la integridad y confidencialidad de los datos personales se garantiza en el apartado 1.f) del artículo 5 del RGPD. Por su parte, la seguridad de los datos personales viene regulada en los artículos 32, 33 y 34 del RGPD, que reglamentan la seguridad del tratamiento, la notificación de una violación de la seguridad de los datos personales a la autoridad de control, así como la comunicación al interesado, respectivamente.

III
Artículo 32 del RGPD

El Artículo 32 *"Seguridad del tratamiento"* del RGPD establece:

"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".

El vector de ataque de la brecha de datos personalesestuvo en la explotación de una vulnerabilidad del puerto 3389 abierto en el servidor para la conexión por escritorio remoto, consiguiendo el atacante acceder al servidor y encriptar todos los ficheros de datos, incluida una base de datos SQL utilizada por el software que usaba la clínica para la gestión de los datos de los pacientes.

En tal momento DENTALCUADROS, no disponía de las medidas de seguridad razonables en función de los posibles riesgos estimados, toda vez que:

- DENTALCUADROS afirma, en su escrito de 10 de octubre de 2023, que *"Con anterioridad al incidente se disponía de antivirus en el ordenador servidor y demás ordenadores, aun así fue posible que se produjera el ataque. Se realizaban copias de seguridad diarias en el ordenador que fue atacado y ocasionalmente en un disco duro externo. El antivirus instalado no pudo evitar la brecha, haciéndonos conscientes de la necesidad de una mayor protección*".

- Por otro lado, el procedimiento de copias de respaldo incorporaba la necesidad de conservar una copia de respaldo en lugar diferente de aquél en que se encuentren los equipos que los tratan para el caso de categorías especiales de datos.

- Y la última copia de seguridad en disco duro externo al propio servidor se había realizado en fecha 14 de marzo de 2023, 37 días antes del ataque; por lo que, no pudieron recuperar los datos de esos días.

Por otro lado, una vez, ocurrida la brecha de datos personales, se implantan las siguientes medidas reactivas:
(…).
Lo que pone de manifiesto que, con anterioridad a la brecha de datos personales, la entidad no contaba con tales medidas de seguridad adecuadas al riesgo.

A tal efecto, se hace necesario traer a colación la sentencia de la Audiencia Nacional de 9 de febrero de 2023 (rec. 770/2022) que dice:

"(…) Las medidas de seguridad implementadas con posterioridad, no afectan a la comisión de la infracción y contrariamente a lo pretendido por la actora no pueden amparar la aplicación de una eximente, (…)".

A mayor abundamiento, en fecha 10 de octubre de 2023, por DENTALCUADROS se adjuntaron cuatro documentos que contienen distintas Evaluaciones de Impacto relativa a la protección de datos (EIPD) de la actividad de tratamiento afectada, realizadas en distintas fechas, un primer documento que contiene la evaluación inicial realizada en el año 2019, y tres documentos adicionales que contienen distintas actualizaciones de la evaluación inicial, realizadas en los años posteriores 2020, 2021 y 2022.

- La primera EIPD, realizada en fecha 19 de diciembre de 2019, incluye un plan de acción que recoge un listado de medidas a implantar para la mitigación de los riesgos, todas estas medidas tienen asignada una fecha como plazo

máximo de implantación, y se afirma: “De acuerdo con el plan de acción y en base a las amenazas detectadas, se proponen las siguientes medidas correctoras que deben implantarse en la organización antes de la fecha indicada en el plazo”. Del listado de medidas destacan:

- ***(…).***

- Del análisis del documento que contiene la segunda EIPD, realizada en fecha 15 de septiembre de 2020, se extrae:

    - Tiene idéntica estructura y contiene información similar (actualizada) a la EIPD realizada en diciembre de 2019.
    - El plan de acción contiene el mismo listado de medidas de seguridad concluidas en la EIPD de 2019, pero en este nuevo documento se ha asignado una nueva fecha como plazo máximo de implantación, 15 de junio de 2021 para las medidas que antes tenían como plazo máximo 19 de septiembre de 2020, y 15 de marzo de 2021 para las medidas con plazo previo 19 de julio de 2020. De esta información se concluye que las medidas no fueron implementadas tras la primera Evaluación de Impacto.

- Del análisis del documento con la tercera EIPD realizada en fecha 15 de julio de 2021, se extrae:

    - Tiene misma estructura y contenido que las anteriores, de su texto no se aprecian diferencias en relación con los riesgos identificados y evaluados, así como tampoco en la relación de medidas incluidas en el plan de acción, únicamente se detecta que se vuelve a cambiar y asignar una nueva fecha máxima de implantación.

- Del análisis del documento con la última EIDP, realizada en fecha 18 de octubre de 2022, se extrae:

    - Tiene similar estructura e información que la última EIPD. El plan de acción incluido contiene idénticas medidas a las aportadas en las evaluaciones anteriores, no obstante, se ha vuelto a cambiar y asignar nuevos plazos máximo de implantación, pasando a tener las nuevas fechas 15 de abril de 2022 y 15 de enero de 2022.

En ningún momento, se ha podido acreditar por DENTALCUADROS la implantación de dichas medidas preventivas, a pesar de la modificación de plazos en las distintas EIPD.

En consecuencia, y por todo lo expuesto, es evidente que DENTALCUADROS no disponía de las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo en el tratamiento de los datos personales del que es responsable.

De conformidad con las evidencias de las que se dispone en este acuerdo de iniciación del procedimiento sancionador, y sin perjuicio de lo que resulte de la

instrucción, se considera que los hechos conocidos podrían ser constitutivos de una infracción, imputable a DENTALCUADROS, por vulneración del artículo 32 del RGPD.

IV
Tipificación de la infracción del artículo 32 del RGPD

La citada infracción del artículo 32 del RGPD supone la comisión de una 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 este respecto, la LOPDGDD, en su artículo 71 *"Infracciones"* establece que *"Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica".*

A efectos del plazo de prescripción, el artículo 73 *"Infracciones consideradas graves"* de la LOPDGDD indica:

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

> *(…)*
>
> *f) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679.*

V
Sanción por la infracción del artículo 32 del RGPD

A efectos de decidir sobre la imposición de una multa administrativa y su cuantía, se considera que la infracción en cuestión es grave a los efectos del RGPD y que procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el artículo 83.2 del RGPD:

Como agravantes:

- b) la intencionalidad o negligencia en la infracción; (artículo 83.2.b) del RGPD);

En este mismo sentido, el Tribunal Supremo viene entendiendo que existe imprudencia siempre que se desatiende un deber legal de cuidado, es decir, cuando el infractor no se comporta con la diligencia exigible. Y en la valoración del grado de diligencia ha de ponderarse especialmente la profesionalidad o no del sujeto, y no cabe duda de que, en el caso ahora examinado, cuando la actividad de la recurrente es de constante y abundante manejo de datos de carácter personal ha de insistirse en el rigor y el exquisito cuidado por ajustarse a las prevenciones legales al respecto. ***[Sentencia de la Audiencia Nacional de 17/10/2007 (rec. 63/2006)]***

- g) las categorías de los datos de carácter personal afectados por la infracción; (artículo 83.2.g) del RGPD).

DENTALCUADROS trata, entre otros, datos personales de salud dental.

El considerando 35 del RGPD establece que *"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".*

La STJUE del caso Lindqvist, de 6 de noviembre de 2003 indica que son datos de salud los previstos en el art. 8.1 de la Directiva 95/46/CE que comprende TODOS los aspectos, tanto físicos como PSIQUICOS de la salud de una persona.

El balance de las circunstancias contempladas en el artículo 83.2 del RGPD y el artículo 76.2 de la LOPDGDD, con respecto a la infracción cometida al vulnerar lo establecido en el artículo 32 del RGPD, permite fijar inicialmente una sanción de 15.000 € (QUINCE MIL EUROS).

VI
Artículo 33 del RGPD

El Artículo 33 "*Notificación de una violación de la seguridad de los datos personales a la autoridad de control*" del RGPD establece:

"1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

3. La notificación contemplada en el apartado 1 deberá, como mínimo:

a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;

b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;
c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;
d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo."

En el presente caso, consta que:

- El 20 de abril de 2023 DENTALCUADROS detectó la brecha al confirmar el cifrado de datos personales que se encontraban recopilados en el servidor.

- El 12 de mayo de 2023 DENTALCUADROS notifica la brecha de datos personales ante la Agencia Española de Protección de Datos.

Por tanto, es evidente que, tal notificación se hizo habiendo transcurrido sobradamente el plazo de las 72 horas previstas en el artículo 33 del RGPD.

Y preguntados por los motivos de la dilación; ya que, en la notificación no se acompañó la indicación de los motivos de la misma, tal y como preceptúa el citado artículo, DENTALCUADROS manifestó, en su escrito de 10 de octubre de 2023, lo siguiente:

"Fueron días de intentar recuperar datos de pacientes para poder seguir trabajando e intentar entender lo que sucedía, por ello la siguiente medida fue presentar la denuncia ante autoridades policiales ya que no sabíamos el alcance de la situación. Es por ello por lo que no sabíamos la necesidad de informar a la AEPD, ya que disponíamos de muy poca información y estábamos pendientes de recopilar datos, siendo esta la primera vez que nos ocurre algo así."

Lo que; en ningún caso, justifica, la dilación en la notificación de la brecha de datos personales a esta Agencia Española de Protección de Datos, pues la ignorancia de las leyes no excusa de su cumplimiento (artículo 6.1 del Código Civil).

De conformidad con las evidencias de las que se dispone en este acuerdo de iniciación del procedimiento sancionador, y sin perjuicio de lo que resulte de la instrucción, se considera que los hechos conocidos podrían ser constitutivos de una infracción, imputable a DENTALCUADROS, por vulneración del artículo 33 del RGPD.

VII
Tipificación de la infracción del artículo 33 del RGPD

De confirmarse, la citada infracción del artículo 33 del RGPD podría suponer 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 este respecto, la LOPDGDD, en su artículo 71 "*Infracciones"* establece que "*Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica".*

A efectos del plazo de prescripción, el artículo 74 *"Infracciones consideradas leves"* de la LOPDGDD indica:

"*Se consideran leves y prescribirán al año las restantes infracciones de carácter meramente formal de los artículos mencionados en los apartados 4 y 5 del artículo 83 del Reglamento (UE) 2016/679 y, en particular, las siguientes:*

> *(…)*
> *m) La notificación incompleta, tardía o defectuosa a la autoridad de protección de datos de la información relacionada con una violación de seguridad de los datos personales de conformidad con lo previsto en el artículo 33 del Reglamento (UE) 2016/679(…).*

VIII
Sanción por la infracción del artículo 33 del RGPD

A efectos de decidir sobre la imposición de una multa administrativa y su cuantía, de conformidad con las evidencias de que se dispone en el presente momento de acuerdo de inicio de procedimiento sancionador, y sin perjuicio de lo que resulte de la instrucción, se considera que la infracción en cuestión es grave a los efectos del RGPD y que procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el artículo 83.2 del RGPD:

Como agravantes:

- g) las categorías de los datos de carácter personal afectados por la infracción; (artículo 83.2.g) del RGPD).

El considerando 35 del RGPD establece que "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".

DENTALCUADROS trata, entre otros, datos personales de salud dental.

El considerando 35 del RGPD establece que *"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".*

La STJUE del caso Lindqvist, de 6 de noviembre de 2003 indica que son datos de salud los previstos en el art. 8.1 de la Directiva 95/46/CE que comprende TODOS los aspectos, tanto físicos como PSIQUICOS de la salud de una persona.

El balance de las circunstancias contempladas en el artículo 83.2 del RGPD y el artículo 76.2 de la LOPDGDD, con respecto a la infracción cometida al vulnerar lo establecido en el artículo 33 del RGPD, permite fijar inicialmente una sanción de 5.000 € (CINCO MIL EUROS).

IX
Adopción de medidas

De confirmarse la infracción, podría acordarse imponer al responsable la adopción de medidas adecuadas para ajustar su actuación a la normativa mencionada en este acto, de acuerdo con lo establecido en el citado artículo 58.2 d) del RGPD, según el cual cada autoridad de control podrá "*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…".* La imposición de esta medida es compatible con la sanción consistente en multa administrativa, según lo dispuesto en el art. 83.2 del RGPD.

Se advierte que no atender la posible orden de adopción de medidas impuestas por este organismo en la resolución sancionadora podrá ser considerado como una infracción administrativa conforme a lo dispuesto en el RGPD, tipificada como infracción en su artículo 83.5 y 83.6, pudiendo motivar tal conducta la apertura de un ulterior procedimiento administrativo sancionador.

Por lo tanto, a tenor de lo anteriormente expuesto, por la Directora de la Agencia Española de Protección de Datos,
SE ACUERDA:

PRIMERO: INICIAR PROCEDIMIENTO SANCIONADOR a DENTALCUADROS BCN S.L.P., con NIF B67480376, por la presunta infracción del Artículo 33 del RGPD y del Artículo 32 del RGPD, tipificadas ambas en el Artículo 83.4 del RGPD.

SEGUNDO: NOMBRAR como instructor/a a ***A.A.A.*** y, como secretario/a, a ***B.B.B.***, indicando que podrán ser recusados, en su caso, conforme a lo establecido en los artículos 23 y 24 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP).

TERCERO: INCORPORAR al expediente sancionador, a efectos probatorios, así como los documentos obtenidos y generados por la Subdirección General de Inspección de Datos en las actuaciones previas al inicio del presente procedimiento sancionador.

CUARTO: 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, sin perjuicio de lo que resulte de la instrucción sería:

- Por la supuesta infracción del artículo 32 del RGPD, tipificada en el artículo 83.4 de dicha norma, multa administrativa de cuantía 15.000,00 euros

- Por la supuesta infracción del artículo 33 del RGPD, tipificada en el artículo 83.4 de dicha norma, multa administrativa de cuantía 5.000,00 euros

QUINTO: NOTIFICAR el presente acuerdo a DENTALCUADROS BCN S.L.P., con NIF B67480376, otorgándole un plazo de audiencia de diez días hábiles para que formule las alegaciones y presente las pruebas que considere convenientes. En su escrito de alegaciones deberá facilitar su NIF y el número de expediente que figura en el encabezamiento de este documento.

Si en el plazo estipulado no efectuara alegaciones a este acuerdo de inicio, el mismo podrá ser considerado propuesta de resolución, según lo establecido en el artículo 64.2.f) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo, LPACAP).

De conformidad con lo dispuesto en el artículo 85 de la LPACAP, podrá reconocer su responsabilidad dentro del plazo otorgado para la formulación de alegaciones al presente acuerdo de inicio; lo que llevará aparejada una reducción de un 20% de la sanción que proceda imponer en el presente procedimiento. Con la aplicación de esta reducción, la sanción quedaría establecida en 16.000,00 euros, resolviéndose el procedimiento con la imposición de esta sanción.

Del mismo modo podrá, en cualquier momento anterior a la resolución del presente procedimiento, llevar a cabo el pago voluntario de la sanción propuesta, lo que supondrá la reducción de un 20% de su importe. Con la aplicación de esta reducción, la sanción quedaría establecida en 16.000,00 euros y su pago implicará la terminación del procedimiento, sin perjuicio de la imposición de las medidas correspondientes.

La reducción por el pago voluntario de la sanción es acumulable a la que corresponde aplicar por el reconocimiento de la responsabilidad, siempre que este reconocimiento de la responsabilidad se ponga de manifiesto dentro del plazo concedido para formular alegaciones a la apertura del procedimiento. El pago voluntario de la cantidad referida en el párrafo anterior podrá hacerse en cualquier momento anterior a la resolución. En este caso, si procediera aplicar ambas reducciones, el importe de la sanción quedaría establecido en 12.000,00 euros.

En todo caso, la efectividad de cualquiera de las dos reducciones mencionadas estará condicionada al desistimiento o renuncia de cualquier acción o recurso en vía administrativa contra la sanción.

En caso de que optara por proceder al pago voluntario de cualquiera de las cantidades señaladas anteriormente (16.000,00 euros o 12.000,00 euros), deberá hacerlo efectivo

mediante su ingreso en la cuenta nº ***IBAN: ES00 0000 0000 0000 0000 0000 (BIC/Código SWIFT: XXXXXXXXXXX)*** abierta a nombre de la Agencia Española de Protección de Datos en la entidad bancaria CAIXABANK, S.A., indicando en el concepto el número de referencia del procedimiento que figura en el encabezamiento de este documento y la causa de reducción del importe a la que se acoge.

Asimismo, deberá enviar el justificante del ingreso a la Subdirección General de Inspección para continuar con el procedimiento en concordancia con la cantidad ingresada.

El procedimiento tendrá una duración máxima de doce meses a contar desde la fecha del acuerdo de inicio. Transcurrido ese plazo sin que se haya dictado y notificado resolución se producirá su caducidad y, en consecuencia, el archivo de actuaciones; de conformidad con lo establecido en el artículo 64 de la LOPDGDD.

En cumplimiento de los artículos 14, 41 y 43 de la LPACAP, se advierte de que, en lo sucesivo, las notificaciones que se le remitan se realizarán exclusivamente de forma electrónica, a través de la Dirección Electrónica Habilitada Única (dehu.redsara.es), y que, de no acceder a ellas, se hará constar su rechazo en el expediente, dando por efectuado el trámite y siguiéndose el procedimiento. Se le informa que puede identificar ante esta Agencia una dirección de correo electrónico para recibir el aviso de puesta a disposición de las notificaciones y que la falta de práctica de este aviso no impedirá que la notificación sea considerada plenamente válida.

Por último, se señala que conforme a lo establecido en el artículo 112.1 de la LPACAP, contra el presente acto no cabe recurso administrativo alguno.

935-18032024

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

>>

SEGUNDO**:** En fecha 1 de mayo de 2024, la parte reclamada ha procedido al pago de la sanción en la cuantía de **12000 euros** haciendo uso de las dos reducciones previstas en el Acuerdo de inicio transcrito anteriormente, lo que implica el reconocimiento de la responsabilidad.

TERCERO**:** El pago realizado, dentro del plazo concedido para formular alegaciones a la apertura del procedimiento, conlleva la renuncia a cualquier acción o recurso en vía administrativa contra la sanción y el reconocimiento de responsabilidad en relación con los hechos a los que se refiere el Acuerdo de Inicio.

FUNDAMENTOS DE DERECHO

I

Competencia

De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada autoridad de control y según lo establecido en los artículos 47, 48.1, 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 (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

Terminación del procedimiento

El artículo 85 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo, LPACAP), bajo la rúbrica "*Terminación en los procedimientos sancionadores*" dispone lo siguiente:

"*1. Iniciado un procedimiento sancionador, si el infractor reconoce su responsabilidad, se podrá resolver el procedimiento con la imposición de la sanción que proceda.*

2. Cuando la sanción tenga únicamente carácter pecuniario o bien quepa imponer una sanción pecuniaria y otra de carácter no pecuniario pero se ha justificado la improcedencia de la segunda, el pago voluntario por el presunto responsable, en cualquier momento anterior a la resolución, implicará la terminación del procedimiento, salvo en lo relativo a la reposición de la situación alterada o a la determinación de la indemnización por los daños y perjuicios causados por la comisión de la infracción.

3. En ambos casos, cuando la sanción tenga únicamente carácter pecuniario, el órgano competente para resolver el procedimiento aplicará reducciones de, al menos, el 20 % sobre el importe de la sanción propuesta, siendo éstos acumulables entre sí. Las citadas reducciones, deberán estar determinadas en la notificación de iniciación del procedimiento y su efectividad estará condicionada al desistimiento o renuncia de cualquier acción o recurso en vía administrativa contra la sanción.

El porcentaje de reducción previsto en este apartado podrá ser incrementado reglamentariamente."

De acuerdo con lo señalado,
la Directora de la Agencia Española de Protección de Datos RESUELVE**:**

PRIMERO: DECLARAR la terminación del procedimiento **EXP202307460**, de conformidad con lo establecido en el artículo 85 de la LPACAP.

SEGUNDO: NOTIFICAR la presente resolución a **DENTALCUADROS BCN S.L.P.**.

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 según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, los interesados podrán interponer 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.

936-040822

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