

Identificación del expediente

Resolución de procedimiento sancionador núm. PS 40/2022, referente a Barnaclínic , SA.

Antecedentes

1. En fecha 19/02/2021, tuvo entrada en la Autoridad Catalana de Protección de Datos un escrito de una persona por el que formulaba denuncia contra Barnaclínic , SA , (en adelante, Barnaclínic) con motivo de un presunto incumplimiento de la normativa sobre protección de datos personales .

En concreto, la persona denunciante exponía que el personal administrativo de la unidad de reproducción asistida (FIVclínic) de Barnaclínic atendía a las personas pacientes en un pasillo ubicado junto a la sala de espera, que era una dependencia abierta donde permanecían el resto de personas pacientes. Añadía que mientras el personal administrativo atendía a la persona paciente se revelaban datos personales, incluidos datos de salud (datos económicos del tratamiento, visitas y pruebas a realizar, procedimientos y estado del proceso de asistencia sanitaria, entre otros), que podían escuchar al resto personas que estaban en la sala de espera. La persona denunciante manifestaba haber sido atendida en fecha 19/02/2021 y que la entidad denunciada le había negado la posibilidad de ser atendida en un despacho cerrado.

Por otra parte, la persona denunciante aportó el testigo de su marido, quien confirmaba los hechos denunciados.

2. La Autoridad abrió una fase de información previa (núm. IP 76/2021), de acuerdo con lo que prevé el artículo 7 del Decreto 278/1993, de 9 de noviembre, sobre el procedimiento sancionador de aplicación a los ámbitos de competencia de la Generalidad, y el artículo 55.2 de la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones públicas (en adelante, LPAC), para determinar si los hechos eran susceptibles motivar la incoación de un procedimiento sancionador.

3. En esta fase de información, en fecha 26/03/2021 se requirió a la entidad denunciada para que informara, entre otras, sobre las medidas que se habían adoptado para evitar que las personas que estaban en la sala de espera, no pudieran escuchar la conversación mantenida por las personas pacientes que son atendidas por el personal administrativo del FIVclínic . Asimismo, se requería a Barnaclínic que aportase copia del análisis de riesgos que se hubiera efectuado.

4. En fecha 13/04/2021, Barnaclínic respondió el requerimiento mencionado a través de escrito en el que exponía lo siguiente:

- Que durante el transcurso de la atención administrativa a las personas pacientes del FIVclínic se revisan los datos demográficos que constan en el sistema, se hacen las explicaciones de las condiciones de pago de los presupuestos, se programan las citaciones, se realizan las gestiones de cobros, etc.
- Que todas las gestiones que se efectúan se enmarcan dentro de la más estricta confidencialidad y con lo relacionado con su asistencia.

- Que durante el mes de diciembre de 2020 y principios del mes de enero de 2021 se llevaron a cabo unas obras de mejora en la Unidad (FIVclínic) , que afectaban, entre ellas, el mostrador de atención a los pacientes.
- Que la intención del nuevo espacio de atención administrativa es poder atender a los pacientes de una forma mucho más personalizada con dos tablas separadas, en lugar de lo que se podía hacer antes con un único mostrador.
- Que dentro del plan de obras estaba previsto la dotación de un sistema de megafonía e hilo musical para la sala de espera para crear un sonido ambiente que permitiría aislar las conversaciones que se mantienen en las tablas de atención a los pacientes. Se estaba a la espera de recibir presupuesto del modelo que se adaptara a sus instalaciones.
- Que siempre que se dispone de un despacho libre en la Unidad, se utiliza para atender a los pacientes. Desgraciadamente no siempre hay disponibilidad y se atiende a los pacientes en el mostrador de administración, como fue el caso de la paciente.

La entidad denunciada adjuntaba en el escrito documentación diversa, pero no el análisis de riesgos requerido.

5. En fecha 28/05/2021 y aún en el marco de esta fase de información previa, la Autoridad llevó a cabo un acto de inspección en las dependencias de la Unidad de Reproducción Asistida (FIVclínic) de Barnaclínic para verificar determinados aspectos organizativos en el ámbito de atención a los pacientes. En ese acto de inspección presencial, los representantes de Barnaclínic manifestaron lo siguiente:

- Que la atención administrativa, siempre que se podía, se realizaba en un despacho cerrado.
- Que cuando no estaba el despacho libre, es cuando se utilizaba el mostrador de atención a los pacientes.
- Que la información que se intercambian las personas administrativas y las pacientes está relacionada con el proceso de reproducción asistida (como fecundación in vitro). Se programan visitas, pruebas, analíticas, ecografías, etc.
- Que las medidas implementadas por la situación de pandemia habían dificultado la atención a los pacientes. En concreto, la paciente debía situarse fuera de la línea roja (en vez de sentarse en una silla más cercana a la persona administrativa) y se había colocado una mampara, lo que conlleva que se deba elevar el tono de voz.
- Que se podía llegar a atender a más de un paciente a la vez en el mostrador de atención a los pacientes, dado que había 2 puestos de atención. Pero lo habitual es que sólo se atendiera a una paciente.
- Que se estaba pendiente de instalar un hilo musical en la sala de espera, para evitar escuchar las conversaciones mantenidas en el mostrador de atención a los pacientes.
- Que no se tenía constancia de si se había realizado un análisis de riesgos para determinar las medidas adecuadas para garantizar la seguridad de los datos que se intercambian en el mostrador de atención a los pacientes.

Asimismo, en esa misma fecha, el personal inspector de la Autoridad verificó lo siguiente:

- Que el espacio de atención a los pacientes estaba compuesto por dos tablas. En el lado interior de cada mesa había un espacio destinado a la persona empleada de la entidad inspeccionada y en el otro lado se situaban las personas pacientes, de pie, fuera de la línea roja que había en el suelo.

- Que el espacio de atención a los pacientes no estaba cerrado. Entre los dos puestos de trabajo ubicados en el mostrador de atención a los pacientes había una mampara de separación (no había sin embargo ninguna separación entre el espacio que ocupaban las personas pacientes atendidas tal y como se constata en las fotografías que efectuó el personal inspector).
- Que la sala de espera estaba ubicada junto al espacio de atención a los pacientes. La sala de espera tampoco era un espacio cerrado. En concreto, no había ningún cierre en la zona de paso entre el pasillo donde se ubicaba el mostrador de atención y la sala de espera.
- Que situado el inspector en la sala de espera, éste pudo escuchar lo que decía la persona auditora de la Autoridad que le acompañaba que estaba ubicada en el espacio de atención a los pacientes. La persona auditora leyó en un tono de voz normal (ni alto ni bajo) un texto, que la persona inspectora entendió completamente. El personal inspector efectuó grabó esta verificación desde el lugar donde se hallaba ubicado éste.

El personal inspector efectuó un reportaje fotográfico del espacio de atención a los pacientes y de la sala de espera.

Por último, el personal inspector requirió a la entidad inspeccionada para que aportara ante la Autoridad copia del análisis de riesgos para determinar las medidas adecuadas para garantizar la seguridad de los datos que se intercambiaban en el mostrador de atención a los pacientes.

6. En fecha 11/06/2021, Barnaclínic aportó copia de un análisis de riesgos efectuado el 10/06/2021.

7. Con fecha 16/06/2021, Barnaclínic confirmó que en fecha 15/06/2021 se había instalado en la sala de espera de FIVclínic un sistema de ambientación musical, que se había comprobado que funcionaba correctamente.

8. En fecha 14/06/2022, la directora de la Autoridad Catalana de Protección de Datos acordó iniciar un procedimiento sancionador contra Barnaclínic por dos presuntas infracciones, ambas previstas en el artículo 83.4.a), en relación con el artículo 32 ; todos ellos del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril, relativo a la protección de las personas físicas en lo que se refiere al tratamiento de datos personales ya la libre circulación de éstas (en adelante, RGPD). Este acuerdo de iniciación se notificó a la entidad imputada en fecha 16/06/2022.

9. En fecha 08/07/2022, Barnaclínic formuló alegaciones al acuerdo de iniciación .

La entidad imputada aportaba con su escrito documentación diversa.

10. En fecha 22/09/2022, la persona instructora de este procedimiento formuló una propuesta de resolución, por la que proponía que la directora de la Autoridad Catalana de Protección de Datos impusiera a Barnaclínic la sanción consistente en una multa de 12.000.- euros (doce mil euros), como responsable de una infracción prevista en el artículo 83.4.a) en relación con el artículo 32.1; y en segundo lugar, la sanción consistente en una multa de 5.000.- euros (cinco mil euros), como responsable de una infracción prevista en el artículo 83.4.a) en relación con el artículo 32.2, todos ellos del 'RGPD.

Esta propuesta de resolución se notificó en fecha 23/09/2022 y se concedía un plazo de 10 días para formular alegaciones.

11. En fecha 07/10/2022, la entidad imputada presentó un escrito en el que reconoce su responsabilidad en los hechos imputados y acreditaba haber efectuado el pago voluntario adelantado de las sanciones pecuniarias que la persona instructora proponía. En este escrito también informaba del traslado de las dependencias del FIVClínic en otra ubicación, a fin de realizar obras de mejora e implementar medidas de seguridad para garantizar la privacidad de las personas pacientes. Y, en fecha 10/10/2022, aportaba copia del nuevo análisis de riesgos efectuado.

Hechos probados

1. Las personas situadas en la sala de espera de la Unidad de Reproducción Asistida (FIVclínic) de Barnaclínic podían acceder al contenido de las conversaciones mantenidas entre el personal administrativo de la entidad y las personas pacientes que eran atendidas en el espacio de atención a los pacientes cercano a la sala de espera, tal y como constató el personal inspector de la Autoridad en fecha 28/05/2021. Entre el espacio de atención al paciente y la sala de espera no había ningún cierre que separara estos dos espacios.

Asimismo, cuando en el espacio de atención a los pacientes se atendía al mismo tiempo a una persona paciente en cada uno de los dos mostradores disponibles, la persona paciente atendida en un mostrador podía escuchar la conversación que mantenía la otra persona paciente atendida en el otro mostrador.

2. Hasta el 10/06/2021, Barnaclínic no había realizado un análisis de riesgos para determinar las medidas técnicas y organizativas apropiadas para garantizar la seguridad de los datos que se intercambiaban en el espacio de atención a los pacientes. En este análisis no se ha tenido en cuenta el riesgo existente cuando se atiende a más de un paciente a la vez en los dos mostradores disponibles en el espacio de atención al paciente del FIVclínic .

Fundamentos de derecho

1. Son de aplicación a este procedimiento lo que prevén la LPAC , y el artículo 15 del Decreto 278/1993, según lo que prevé la DT 2a de la Ley 32/2010, de 1 de octubre, de Autoridad Catalana de Protección de Datos. De conformidad con los artículos 5 y 8 de la Ley 32/2010, la resolución del procedimiento sancionador corresponde a la directora de la Autoridad Catalana de Protección de Datos. La entidad imputada, Barnaclínic , es una entidad comprendida dentro del ámbito de actuación de esta Autoridad conforme al artículo 3.e) de la Ley 32/2010, de 1 de octubre.

2. De conformidad con el artículo 85.3 de la LPAC, tanto el reconocimiento de responsabilidad como el pago voluntario adelantado de la sanción pecuniaria propuesta conllevan la aplicación de unas reducciones. La efectividad de estas reducciones está condicionada al desistimiento o renuncia de cualquier acción o recurso por vía administrativa contra la sanción. Para ambos casos, los apartados 1 y 2 del artículo 85 de la LPAC contemplan la terminación del procedimiento.

Aunque presentó alegaciones en el acuerdo de iniciación, la entidad imputada no ha formulado alegaciones a la propuesta de resolución, ya que se ha acogido a ambas

opciones para reducir el importe de la sanción. Sin embargo, se considera oportuno reiterar a continuación lo más relevante de la respuesta motivada que la persona instructora dio a las alegaciones ante el acuerdo de iniciación.

2.1. Sobre el hecho probado primero.

Del 1r apartado de su escrito de alegaciones ante el acuerdo de iniciación, se infería que la entidad imputada concretaba que el personal de Barnaclínic que atendía a las personas pacientes no era personal sanitario, sino personal administrativo, apreciación que se recogió en el apartado de hechos probados de la propuesta de resolución y también se ha recogido en el mismo apartado de esta resolución.

Dicho esto, también indicaba que en el marco de la información previa no constaba acreditado que el personal de Barnaclínic que atendía a las personas pacientes en el mostrador de atención facilitaran información clínica u otros datos personales. Añadía que la información asistencial sólo se facilitaba en los consultorios médicos.

Pues bien, tal y como señalaba la persona instructora en la propuesta de resolución, al margen de que la persona denunciante (cliente de la Unidad FIVClínic) manifestaba que mientras el personal administrativo atendía a la persona paciente se revelaban datos personales, incluidos datos de salud; debía tenerse en cuenta que mediante escrito de 13/04/2021, la entidad imputada admitió que en dicho mostrador se revisaban los datos demográficos que constaban en el sistema o se programaban las citaciones, entre otros. Asimismo, las personas representantes de Barnaclínic en el acto de inspección presencial efectuado el 28/05/2021 en la Unidad FIVClínic (entre ellas, la persona que suscribía el escrito de alegaciones ante el acuerdo de iniciación) manifestaron que la información que se intercambian las personas administrativas y las pacientes, estaba relacionada con el proceso de reproducción asistida (como fecundación in vitro); y que se programaban visitas, pruebas, analíticas, ecografías, etc.

También en su escrito de alegaciones ante el acuerdo de iniciación la entidad imputada indicaba que en el punto de gestión administrativa se gestionaba el calendario de citas (visitas y pruebas) o se gestionaba el proceso asistencial (de reproducción asistida). A su vez, aparte de la información que proporcionara el personal de FIVClínic también debía tenerse presente que las personas pacientes podían facilitar datos personales, incluidos datos de salud.

En este punto, procede acudir el artículo 4.15) del RGPD que define los datos relativos a la salud como los datos personales relativos *“a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria , que revelan información sobre su estado de salud ”*.

A su vez, el considerante 35 del RGPD dispone lo siguiente en relación a los datos relativos a la salud:

“Entre los datos personales relativos a la salud se deben incluir todas las datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasado , presente o futuro . Se incluye la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria , o con ocasión de la prestación de tal

asistencia , de conformidad con la Directiva 2011/24/UE del Parlamento Europeo y del Consejo (1); todo número, símbolo o fecha asignado a una persona física que la identifique de manera unívoca a efectos sanitarios ; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas , y cualquier información relativa, a título de ejemplo , a una enfermedad , una discapacidad , el riesgo de padecer enfermedades , el historial médico , el tratamiento clínico o el estado fisiológico o biomédico del interesado , independientemente de su fuente , por ejemplo un médico u otro profesional sanitario , un hospital, un dispositivo médico , o una prueba diagnóstica in vitro.”

De conformidad con lo anterior, tal y como indicaba la persona instructora, debe concluirse que las personas pacientes y el personal de Barnaclínic que presta servicios en el mostrador de la Unidad FIVClínic , se intercambiaban datos relativos a la salud de ésta . A modo de ejemplo, la programación de visitas médicas, pruebas, analíticas o ecografías tienen tal consideración de datos relativos a la salud.

Por último, cabe poner de manifiesto que aunque la entidad imputada negaba que se faciliten datos personales en el mostrador, indicaba que se habían aplicado medidas técnicas y organizativas para salvaguardar la confidencialidad de las personas pacientes minimizando riesgos y garantizando la privacidad sobre las referencias personales de acuerdo a la privacidad desde el diseño y por defecto del artículo 25 y con las medidas adecuadas de acuerdo al artículo 32, ambos del RGPD.

Por tanto, tal y como concluía la persona instructora, no se puede admitir que en el mostrador de atención no se intercambiaban datos personales, incluyendo datos de salud.

Asimismo, cabe concluir que las conversaciones mantenidas entre el personal del mostrador y las personas pacientes, podían ser escuchadas tanto por las personas que se ubican en la sala de espera, como también por la persona que podía ser atendida simultáneamente en el otro lugar de atención del mostrador (el mostrador de atención consta de 2 puestos de atención).

En este sentido, en la propuesta de resolución se remarcó que en su escrito de alegaciones ante el acuerdo de iniciación, la entidad imputada admitía que se había previsto “ *la instalación de hilo musical como medida técnica para que actúe como barrera acústica evitando el acceso a las conversaciones desde la sala de espera*”. Así pues, Barnaclínic era consciente de que se podían escuchar las conversaciones desde la sala de espera y previó una medida para evitarlo, que no se adoptó hasta el 15/06/2021 (con posterioridad al acto de inspección presencial de 28/05/2022).

2.2. Sobre el probado segundo.

Seguidamente, la entidad imputada admitía en su escrito de alegaciones ante el acuerdo de iniciación que “*el análisis de riesgo se ha efectuado si bien no formal si de facto*” .

A tal efecto, invocaba que efectuó un proyecto de obras para mejorar los espacios de atención administrativa en relación con la sala de espera, que contemplaba “ *un cambio significativo en la disposición y cierre de los puntos de atención administrativa, el traslado*

del box de enfermería y la instalación de hilo musical como medida técnica para que actúe como barrera acústica evitando el acceso a las conversaciones desde la sala de espera.”

Por motivos obvios, este proyecto de obra no podía calificarse como un análisis de riesgos en cuanto al tratamiento de datos personales.

Cierto, como indicaba la entidad imputada en su escrito de alegaciones ante el acuerdo de iniciación, que la normativa de protección de datos no establecía una metodología para efectuar un análisis de riesgos, pero también lo es que artículo 5.2 del RGPD que regula el principio de responsabilidad proactiva, dispone que el responsable del tratamiento es responsable de que se cumpla los principios establecidos en el artículo 5.1 del RGPD (entre ellos, el principio de integridad) y que debe poder demostrarlo.

Cabe decir que en el marco de las actuaciones de información previa, en fecha 26/03/2021, se requirió a la entidad imputada para que aportara la copia del análisis de riesgos que se hubiera efectuado y que éste no se aportó.

Asimismo, en el acto de inspección presencial efectuado el 28/05/2021, las personas representantes de Barnaclínic (entre ellas, la persona delegada de protección de datos de Barnaclínic) manifestaron que no tenían constancia de que se hubiera efectuado un análisis de riesgos para determinar las medidas adecuadas para garantizar la seguridad de los datos que se intercambian en el mostrador de atención a los pacientes. Ante esta manifestación, el personal inspector requirió Barnaclínic para que aportara ante la Autoridad copia del análisis de riesgos. En respuesta a este requerimiento, en fecha 11/06/2021, se aportó el análisis de riesgos efectuado el 10/06/2021.

Por otra parte, la entidad imputada aducía que disponía de un Manual de Buenas Prácticas a disposición de los empleados en el que se regulaba adecuadamente el deber de confidencialidad y que se había hecho formación al personal. A este respecto, tal y como se precisaba en la propuesta de resolución, basta remarcar que la infracción vinculada al hecho probado según se refería a la falta de un análisis de riesgos para determinar las medidas de seguridad.

2.3. Sobre el principio “*non bis in idem*” .

Barnaclínic exponía también en su escrito de alegaciones, que la calificación jurídica hecha en el escrito del acuerdo de iniciación *“lleva a imputar dos veces un mismo hecho con dos infracciones graves, ambas bajo el mismo tipo legal del artículo 73.f) de la LOPDiGDD , por falta de adopción de medidas técnicas y organizativas para garantizar un nivel de seguridad.”* Y añadía que había identidad en el hecho, puesto que sin análisis no habría medidas, en el sujeto y en el fundamento.

Tal y como señalaba la persona instructora en la propuesta de resolución, en el presente caso no se vulnera el principio de *non bis in idem* o concurrencia de sanciones. Este principio constituye una de las garantías de la legalidad sancionadora (art. 25 CE) y consiste en impedir que pueda sancionarse dos veces cuando se aprecie identidad de sujeto, hechos y fundamentos. El principio de *non bis in idem* se encuentra recogido en el artículo 102 de la Ley 26/2010, de 3 de agosto, de régimen jurídico y de procedimiento de las administraciones públicas de Cataluña, y en el artículo 31 de la Ley 40 /2015, de 1 de octubre, de régimen jurídico del sector público, que establece que *“ No se pueden sancionar los hechos que lo*

hayan sido penal o administrativamente, en los casos en que se aprecie identidad del sujeto, hecho y fundamento.”

En el presente caso, no existe identidad de hecho, ni de fundamento entre las dos sanciones imputadas. Por un lado, se sanciona el hecho de no aplicar medidas de seguridad para garantizar que terceras personas no autorizadas podían acceder a datos personales, lo que infringe el artículo 32.1 del RGPD, que establece una obligación de resultado. Y por otra, se sanciona no disponer de un análisis de riesgos, lo que contraviene el artículo 32.2 del RGPD, que establece una obligación formal.

2.4. Acerca del régimen sancionador.

Por último, Barnaclínic exponía en su escrito de alegaciones ante el acuerdo de iniciación que es una entidad que está vinculada al Hospital Clínic de Barcelona y que, si está dentro del ámbito de actuación del Autoridad, debe aplicarse el régimen sancionador previsto en el artículo 77 de la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (en adelante, LOPDGDD).

Pues bien, tal y como admitía la entidad imputada, Barnaclínic es una sociedad privada, lo que no se ve alterado por el hecho de que su capital pueda ser de titularidad pública.

Dado que las empresas privadas no se incluyen entre las entidades enumeradas en el artículo 77.1 de la LOPDFFF, no se puede aplicar el régimen sancionador de amonestación previsto para estas entidades. En el caso concreto de las entidades del artículo 77.1.c) de la LOPDFFF (la Administración General del Estado, las administraciones de las comunidades autónomas y las entidades que integran la Administración local), que invocaba la entidad imputada, es suficiente señalar que tanto el artículo 2 de la Ley 39/2015, como el artículo 2 de la Ley 40/2015, diferencian a las entidades descritas en el artículo 77.1.c) de la LOPDFFF, de las entidades de derecho privado vinculadas o dependientes de las administraciones públicas.

3. En relación con los hechos descritos en el punto primero del apartado de hechos probados, es necesario acudir al artículo 5.1.f) del RGPD, que regula el principio de integridad y de confidencialidad determinante que los datos personales serán *“ tratados de tal modo 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 ”*.

Por su parte, el artículo 32.1 del RGPD, en lo referente a la seguridad de los datos, dispone lo siguiente:

“1. Teniendo en cuenta el estado de la técnica , los costes de aplicación , y la naturaleza , el alcance , el contexto y las 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 las 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 .*

Durante la tramitación de este procedimiento se ha acreditado debidamente el hecho descrito en el punto 1º del apartado de hechos probados, que es constitutivo de la infracción prevista en el artículo 83.4.a) del RGPD, que tipifica como tal la vulneración de “*las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43*”, entre las que se encuentran las previstas en el artículo 32.1 y 32.2 del RGPD.

La conducta que aquí se aborda se ha recogido como infracción grave en el artículo 73.f) de la LOPDDDD, en la siguiente forma:

"f) La falta de adopción de las medidas técnicas y organizativas que sean apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos que exige el artículo 32.1 del Reglamento (UE) 2016/679."

4. Con respecto al hecho descrito en el punto 2 del apartado de hechos probados, también es necesario acudir al artículo 5.1.f) del RGPD, que regula el principio de integridad y de confidencialidad .

Asimismo, el artículo 32.2 del RGPD establece que:

"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 ."

Y el artículo 28.1 del LOPDDDD determina lo siguiente:

"1. Los responsables y encargados, teniendo en cuenta los elementos que enumeran los artículos 24 y 25 del Reglamento (UE) 2016/679, deben determinar las medidas técnicas y organizativas apropiadas que deben aplicar con el fin de garantizar y acreditar que el tratamiento es conforme al citado Reglamento, a esta Ley Orgánica, sus normas de desarrollo y la legislación sectorial aplicable. En particular deben valorar si procede realizar la evaluación de impacto en la protección de datos y la consulta previa a que se refiere la sección 3 del capítulo IV del Reglamento mencionado."

De conformidad con lo expuesto, el hecho recogido en el punto 2 del apartado de hechos probados constituye la infracción prevista en el artículo 83.4.a) el RGPD, antes transcrita.

A su vez, esta conducta se ha recogido como infracción grave en el artículo 73.p) de la LOPDDDD, en la siguiente forma:

"p) El tratamiento de datos personales sin llevar a cabo una valoración previa de los elementos mencionados en el artículo 28 de esta Ley orgánica."

5. Al tratarse Barnaclínic, de una entidad de derecho privado, resulta de aplicación el régimen sancionador general previsto en el artículo 83 del RGPD.

El artículo 83.4 del RGPD prevé para las infracciones allí previstas, se sancionen con una multa administrativa de 10.000.000 de euros 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.

En relación con la conducta descrita en el apartado 1º de hechos probados, según lo establecido en el artículo 83.2 del RGPD, así como de conformidad con el principio de proporcionalidad consagrado en el artículo 29 de la Ley 40/2015, tal y como indicaba la persona instructora en la propuesta de resolución, procede imponer la sanción de 12.000 euros (doce mil euros). Esta cuantificación de la multa se basa en la ponderación entre los criterios agravantes y atenuantes que a continuación se indican.

Como criterios atenuantes, se observa la concurrencia de las siguientes causas:

- La falta de intencionalidad (art. 83.2.b).
- El hecho de que no consta que Barnaclínic hubiera cometido ninguna infracción con anterioridad (art. 83.2.e RGPD).
- La actitud proactiva y cooperadora con la Autoridad con el fin de remediar la infracción y mitigar sus posibles efectos adversos (art. 83.2.f RGPD). Al respecto cabe decir que consta que Barnaclínic adoptó medidas para remediar la infracción, como instalar un hilo musical para evitar que desde la sala de espera se puedan escuchar las conversaciones que se mantenían en el mostrador de atención (y en fecha 07/10/2022 ha informado que dicho mostrador ha dejado de ser operativo).
- La adhesión de Barnaclínic al código de tipos de la Unión Catalana de Hospitales (art. 83.2.j RGPD).
- La falta de beneficios obtenidos como consecuencia de la comisión de la infracción (art. 83.2.k RGPD y art. 76.2.c LOPDGDD).

Por el contrario, como criterios agravantes, hay que tener en cuenta los siguientes elementos :

- La infracción afectaba a categorías especiales de datos (art. 83.2.g RGPD).
- La vinculación de la actividad del infractor (centro sanitario) con la práctica de tratamientos de datos personales (art. 83.2.k RGPD y art. 76.2.b LOPDGDD).

Y, en cuanto a la conducta descrita en el apartado 2º de hechos probados, tal como indicaba la persona instructora en la propuesta de resolución, imponer la sanción de 5.000 euros (cinco mil euros). Esta cuantificación de la multa se basa en la ponderación entre los criterios agravantes y atenuantes que a continuación se indican.

Como criterios atenuantes, se observa la concurrencia de las siguientes causas:

- El hecho de que no consta que Barnaclínic hubiera cometido ninguna infracción con anterioridad (art. 83.2.e RGPD).

- La actitud proactiva y cooperadora con la Autoridad con el fin de remediar la infracción y mitigar sus posibles efectos adversos (art. 83.2.f RGPD). Al respecto cabe decir que consta que Barnaclínic adoptó medidas para remediar la infracción y, en concreto, efectuó en fecha 10/06/2021 un análisis de riesgos.
- La adhesión de Barnaclínic al código de tipos de la Unión Catalana de Hospitales (art. 83.2.j RGPD).
- La falta de beneficios obtenidos como consecuencia de la comisión de la infracción (art. 83.2.k RGPD y art. 76.2.c LOPDGDD).

Por el contrario, como criterios agravantes, hay que tener en cuenta los siguientes elementos :

- La vinculación de la actividad del infractor (centro sanitario) con la práctica de tratamientos de datos personales (art. 83.2.k RGPD y art. 76.2.b LOPDGDD).

6. Por otra parte, de conformidad con el artículo 85.3 de la LPAC y tal y como se adelantaba al acuerdo de iniciación, si antes de la resolución del procedimiento sancionador la entidad imputada reconoce su responsabilidad o hace el pago voluntario de la sanción pecuniaria, procede aplicar una reducción del 20% sobre el importe de la sanción provisionalmente cuantificada. Si concurren los dos casos mencionados, la reducción se aplicará de forma acumulada (40%).

Como se ha avanzado, la efectividad de dichas reducciones está condicionada al desistimiento o renuncia de cualquier acción o recurso por vía administrativa contra la sanción (art. 85.3 de la LPAC, in *fine*) .

Pues bien, tal y como se ha indicado en los antecedentes, mediante escrito de 07/10/2022, la entidad imputada ha reconocido su responsabilidad. Asimismo, en la misma fecha ha abonado de forma avanzada 10.200 euros (diez mil doscientos euros), correspondientes a la cuantía de las sanciones resultantes una vez aplicada la reducción acumulada del 40%.

7. Ante la constatación de las infracciones previstas en el art. 83 del RGPD en relación con ficheros o tratamientos de titularidad privada, el artículo 21.3 de la Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos, faculta a la directora de la Autoridad para que la resolución que declara la infracción establezca las medidas oportunas para que cesen o se corrijan sus efectos.

Pues bien, por medio de escrito de 07/10/2022, la entidad imputada manifiesta que ha cerrado provisionalmente el espacio donde se ubicaba el FIVclínic (el servicio se presta en otra ubicación diferente), para realizar obras de mejora e implementar medidas de seguridad para garantizar la privacidad de las personas pacientes. Asimismo, señala que el proyecto contempla la atención en despachos de forma personalizada. Por otra parte, a fecha 10/10/2022 también aporta un nuevo análisis de riesgos.

Dado lo anterior, no procede requerir ninguna medida correctora en el bien entendido que la sala de atención a los pacientes del FIVclínic objeto del presente procedimiento sancionador ha dejado de ser operativa.

Por todo esto, resuelvo:

1. Imponer a Barnaclínic , SA, en primer lugar, la sanción consistente en una multa de 12.000.- euros (doce mil euros), como responsable de una infracción prevista en el artículo 83.4.a) en relación con el artículo 32.1 ; y en segundo lugar, la sanción consistente en una multa de 5.000.- euros (cinco mil euros), como responsable de una infracción prevista en el artículo 83.4.a) en relación con el artículo 32.2, todos ellos del 'RGPD.

No es necesario requerir medidas correctoras para corregir los efectos de la infracción, de conformidad con lo expuesto en el fundamento de derecho 7º.

2. Declarar que Barnaclínic , SA ha hecho efectivo el pago adelantado de 10.200 euros (diez mil doscientos euros), que corresponde al importe total de las dos sanciones impuestas, una vez aplicado el porcentaje de deducción del 40% correspondiente a las reducciones previstas en el artículo 85 de la LPAC.

3. Notificar esta resolución a Barnaclínic .

4. Ordenar que se publique esta resolución en la web de la Autoridad (apdcat.gencat.cat) , de conformidad con el artículo 17 de la Ley 32/2010, de 1 de octubre.

Contra esta resolución, que pone fin a la vía administrativa de acuerdo con los artículos 26.2 de la Ley 32/2010, de 1 de octubre, de la Autoritat Catalana de Protecció de Dades, y 14.3 del Decreto 48/2003 , de 20 de febrero, por el que se aprueba el Estatuto de la Agencia Catalana de Protecció de Dades, la entidad imputada puede interponer, con carácter potestativo, un recurso de reposición ante la directora de la Autoritat Catalana de Protecció de Dades, en el plazo de un mes a contar desde el día siguiente de su notificación, de acuerdo con lo que prevén el artículo 123 y siguientes de la LPAC. También puede interponer directamente un recurso contencioso administrativo ante los Juzgados de lo Contencioso-Administrativo, en el plazo de dos meses a contar desde el día siguiente de su notificación, de acuerdo con los artículos 8, 14 y 46 de la Ley 29/1998, de 13 de julio, reguladora de la jurisdicción contencioso-administrativa.

Si la entidad imputada manifiesta a la Autoridad su intención de interponer recurso contencioso administrativo contra la resolución firme en vía administrativa, la resolución se suspenderá cautelarmente en los términos previstos en el artículo 90.3 de la LPAC.

Igualmente, la entidad imputada podrá interponer cualquier otro recurso que estime conveniente para defender sus intereses.

La directora,