- **Expediente Nº: EXP202204816**

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 13 de junio de 2023, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a ***INSTITUT MARQUÉS OBSTETRICIA I GINECOLOGIA, S.L.P.*** (en adelante, la parte reclamada), mediante el Acuerdo que se transcribe:

<<

Expediente N.º: EXP202204816
IMI Reference: A56ID 406200 Case Register 434041

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 18 de abril de 2022, la Subdirección General de Inspección de Datos (SGID) recibió para su valoración un escrito de notificación de brecha de seguridad de datos personales remitido por **INSTITUT MARQUÉS OBSTETRICIA I GINECOLOGIA, S.L.P.** con NIF B62187323 (en adelante, **INSTITUTO MARQUÉS** o "la entidad notificante"), con entrada en esta Agencia el 24 de diciembre de 2021, en el que informa a la Agencia Española de Protección de Datos de lo siguiente:

Brecha de disponibilidad por ciberataque con posibles consecuencias para los afectados. Hay indicios de que datos extraídos por la brecha han sido utilizados para el envío de correos electrónicos a los afectados.

Fecha de detección de la brecha: 21 de diciembre de 2021.

Indican que han comunicado la brecha a los afectados el día 29 de marzo de 2022 a consecuencia del conocimiento, el día 25 de marzo de 2022, de que sí que había sido afectada la confidencialidad de los datos. Tuvieron conocimiento de esto debido a que la entidad notificante recibió un correo electrónico desde la cuenta ******URL.1*** que contenían sus propios datos extraídos de los sistemas de información de la entidad notificante.

Existen afectados en otros países: Francia, Irlanda, Italia, Rumanía y Reino Unido.

Número de afectados según notificación: 400 usuarios, pacientes y empleados.
Tipología de los datos según notificación: Datos de identidad, imagen, datos de contacto, datos económicos y de medios de pago, y datos de salud y genéticos.

SEGUNDO: A través del "Sistema de Información del Mercado Interior" (en lo sucesivo Sistema IMI), regulado por el Reglamento (UE) nº 1024/2012, del Parlamento Europeo y del Consejo, de 25 de octubre de 2012 (Reglamento IMI), cuyo objetivo es favorecer la cooperación administrativa transfronteriza, la asistencia mutua entre los Estados miembros y el intercambio de información, en fecha 6 de junio de 2022, esta Agencia se declaró autoridad principal en el presente asunto. El traslado de esta cuestión se realiza de conformidad con lo establecido en el artículo 56 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27/04/2016, relativo a la Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y a la Libre Circulación de estos Datos (en lo sucesivo, RGPD), teniendo en cuenta su carácter transfronterizo y que esta Agencia es competente para actuar como autoridad de control principal, dado que INSTITUTO MARQUÉS tiene su sede social y establecimiento en España.

Los tratamientos de datos que se llevan a cabo afectan a interesados en varios Estados miembros. Según las informaciones incorporadas al Sistema IMI, de conformidad con lo establecido en el artículo 60 del RGPD, actúa en calidad de "autoridad de control interesada", la autoridad de Italia, en virtud del artículo 4.22 del RGPD, dado que los interesados que residen en el territorio de esta autoridad de control se ven sustancialmente afectados o es probable que se vean sustancialmente afectados por el tratamiento objeto del presente procedimiento.

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 RGPD, y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), teniendo conocimiento de los siguientes extremos:

Respecto de la empresa

La entidad notificante es una sociedad limitada de nacionalidad española. Según los datos obrantes en AXESOR se trata de una matriz de grupo con 115 empleados y un volumen de ventas de 9.684.025 euros. No se han encontrado en los sistemas de información de esta Agencia expedientes anteriores al presente con relación a brechas de esta entidad.

Se ha solicitado información y documentación a la entidad notificante, y de la respuesta recibida el 27 de junio de 2022, junto con la información aportada en las notificaciones de la brecha realizadas los días 24 de diciembre de 2021, 15 de febrero de 2022 y 30 de marzo de 2022, se desprende lo siguiente:

Respecto de la cronología de los hechos. Acciones tomadas con objeto de minimizar los efectos adversos y medidas adoptadas para su resolución final

(…).

(…).

(…).

(…).

(…).

(…).

(…).

(…).

(…):

(…)

"(…)."

(…):

(…)

(…).

(…).

(…).

(…):

(…)

(…).

(…).

(…).

(…)

Respecto del contrato de encargado del tratamiento

(…):

- (…).

- ***"(…)."***

- (…).

- "(…)".

Respecto de las medidas de seguridad implantadas

(…):

(…)

(…)

(…).

(…)

(…).

CUARTO: Con fecha 21 de marzo de 2023, la Directora de la AEPD adoptó un proyecto de decisión de inicio de procedimiento sancionador. Siguiendo el proceso establecido en el artículo 60 del RGPD, el 31 de marzo de 2023 se transmitió a través del sistema IMI este proyecto de decisión y se les hizo saber a las autoridades interesadas que tenían cuatro semanas desde ese momento para formular objeciones pertinentes y motivadas. El plazo de tramitación del presente procedimiento sancionador quedó suspendido automáticamente durante estas cuatro semanas, de acuerdo con lo dispuesto en el artículo 64.4 de la LOPDGDD.

Dentro del plazo a tal efecto, las autoridades de control interesadas no presentaron objeciones pertinentes y motivadas al respecto, por lo que se considera que todas las autoridades están de acuerdo con dicho proyecto de decisión y están vinculadas por este, de conformidad con lo dispuesto en el apartado 6 del artículo 60 del RGPD.

Este proyecto de decisión, que se notificó a INSTITUTO MARQUÉS conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP), fue recogido en fecha 22 abril de 2023, como consta en el acuse de recibo que obra en el expediente.

FUNDAMENTOS DE DERECHO

I

Competencia y normativa aplicable

De acuerdo con lo dispuesto en los artículos 58.2 y 60 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD), y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 y 68.2 de la 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
Cuestiones previas

En el presente caso, de acuerdo con lo establecido en el artículo 4.1 y 4.2 del RGPD, consta la realización de un tratamiento de datos personales, toda vez que INSTITUTO MARQUÉS realiza la recogida y conservación de, entre otros, los siguientes datos personales de personas físicas: datos de identidad, imagen, datos de contacto, datos económicos y de medios de pago, y datos de salud y genéticos, entre otros tratamientos.

INSTITUTO MARQUÉS 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. Además, se trata de un tratamiento transfronterizo, dado que INSTITUTO MARQUÉS está establecida en España, si bien presta servicio a otros países de la Unión Europea.

El RGPD dispone, en su artículo 56.1, para los casos de tratamientos transfronterizos, previstos en su artículo 4.23), en relación con la competencia de la autoridad de control principal, que, sin perjuicio de lo dispuesto en el artículo 55, la autoridad de control del establecimiento principal o del único establecimiento del responsable o del encargado del tratamiento será competente para actuar como autoridad de control principal para el tratamiento transfronterizo realizado por parte de dicho responsable o encargado con arreglo al procedimiento establecido en el artículo 60. En el caso examinado, como se ha expuesto, INSTITUTO MARQUÉS tiene su establecimiento en España, por lo que la Agencia Española de Protección de Datos es la competente para actuar como autoridad de control principal.

Por su parte, el artículo 4 apartado 12 del RGPD define, de un modo amplio, las "*violaciones de seguridad de los datos personales*" (en adelante brecha de seguridad) 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 seguridad de datos personales en las circunstancias arriba indicadas, categorizada como una brecha de confidencialidad y

de disponibilidad, al haberse accedido indebidamente a los datos personales de, al menos, 400 usuarios, y haber quedado inaccesibles los datos personales de estos usuarios, desde el día 21 de diciembre de 2021.

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
Deber de confidencialidad

El artículo 5.1.f) "Principios relativos al tratamiento" del RGPD establece:

"*1. Los datos personales serán*:
(…)

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

En el presente caso, consta que los datos personales de más de 400 usuarios, obrantes en la base de datos de INSTITUTO MARQUÉS, fueron accedidos por un tercero como producto de la brecha de seguridad sufrida.

De conformidad con las evidencias de las que se dispone en este acuerdo de inicio de 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 INSTITUTO MARQUÉS, por vulneración del artículo 5.1.f) del RGPD.

IV
Tipificación y calificación de la infracción del artículo 5.1.f) del RGPD

De confirmarse, la citada infracción del artículo 5.1.f) del RGPD podría suponer la comisión de las infracciones tipificadas en el artículo 83.5 del RGPD que bajo la rúbrica "*Condiciones generales para la imposición de multas administrativas*" dispone:

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

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

A 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 72 "*Infracciones consideradas muy graves*" de la LOPDGDD indica:

"*1. En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes*:

a) El tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 del Reglamento (UE) 2016/679. (…)"

V

Propuesta de sanción por la infracción del artículo 5.1.f) 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 procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el artículo 83.2 del RGPD:

Como agravantes:

- La naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate, así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido (apartado a): por el acceso indebido a datos de salud especialmente protegidos de al menos 400 afectados, desde el 21 de diciembre de 2021 al 25 de marzo de 2022, como mínimo.

- Las categorías de los datos de carácter personal afectados por la infracción (apartado g): En el presente supuesto, de acuerdo con la notificación de la entidad, se habrían visto expuestos datos de origen racial, salud, genéticos, entre otros datos personales de los afectados.

Como atenuantes:

- Cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción (apartado k): se adoptó una serie de medidas, tales como el ***(…)***, entre otras.

Asimismo, se considera que procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el apartado 2 del artículo 76 "*Sanciones y medidas correctivas*" de la LOPDGDD:

- La vinculación de la actividad del infractor con la realización de tratamientos de datos personales (apartado b): se trata de una entidad habituada al tratamiento de datos personales de salud.

Como atenuantes:

- Disponer, cuando no fuere obligatorio, de un delegado de protección de datos (apartado g).

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 5.1.f) del RGPD, permite fijar inicialmente una sanción de 50.000 € (cincuenta mil euros).

VI
Medidas de seguridad

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".

En el presente caso, en el momento de producirse la brecha, consta la existencia de indicios razonables y suficientes de que las medidas de seguridad, tanto de índole técnica como organizativas, con las que contaba INSTITUTO MARQUÉS en relación con los datos que sometía a tratamiento, no eran las adecuadas.

Dado que la empresa trata datos de salud, raza, entre otros, por tratarse de datos especialmente protegidos cuya vulneración implicaría un riesgo mayor para los derechos y libertades de los individuos, se supone un riesgo añadido que se ha de valorar y que aumenta la exigencia del grado de protección en relación con la seguridad y salvaguarda de la integridad y confidencialidad de estos datos.

Este riesgo debe ser tenido en cuenta por el responsable del tratamiento que, en función de este, debe establecer las medidas técnicas y organizativas necesarias que impidan la pérdida de control de los datos por parte del responsable del tratamiento y, por tanto, por parte de los titulares de los datos que se los proporcionaron.

De los hechos descritos no consta que, INSTITUTO MARQUÉS, como responsable del tratamiento ahora analizado haya dispuesto de las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, por lo menos en lo que respecta al ***(…)*** de la empresa.

De conformidad con las evidencias de las que se dispone en este acuerdo de inicio de 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 INSTITUTO MARQUÉS, por vulneración del artículo 32 del RGPD.

VII

Tipificación y calificación de la infracción del artículo 32 del RGPD

De confirmarse, la citada infracción del artículo 32 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 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". (…)

VIII
Propuesta de sanción por la infracción del artículo 32 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 procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el artículo 83.2 del RGPD:

Como agravantes:

- La naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido (apartado a): por no contar con las medidas de seguridad adecuadas, lo cual posibilitó que los datos de al menos 400 interesados se vieran afectados por una brecha como la del presente caso, que posibilitó la vulneración de la confidencialidad de estos datos de salud desde el día 21 de diciembre de 2021 a 25 de marzo de 2022 y la indisponibilidad de parte de estos datos, desde el día 21 de diciembre de 2021 a la actualidad.

- Las categorías de los datos de carácter personal afectados por la infracción (apartado g): En el presente supuesto, de acuerdo con la notificación de la entidad, se habrían visto comprometidos datos de origen racial, salud, genéticos, entre otros datos personales de los afectados.

Como atenuantes:

- Cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción(apartado k): la empresa tenía adoptada una serie de medidas (si bien, insuficientes) para evitar que una brecha de seguridad tuviera lugar y, a posteriori, adoptó también medidas para mejorar sus sistemas de seguridad tales como ***(…)***, entre otras.

Asimismo, se considera que procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el apartado 2 del artículo 76 "*Sanciones y medidas correctivas*" de la LOPDGDD:

- La vinculación de la actividad del infractor con la realización de tratamientos de datos personales (apartado b): se trata de una entidad habituada al tratamiento de datos personales de salud.

Como atenuantes:

- Disponer, cuando no fuere obligatorio, de un delegado de protección de datos (apartado g):

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 20.000 € (veinte mil euros).

IX
Comunicación de una violación de la seguridad

El artículo 34 "*Comunicación de una violación de la seguridad de los datos personales al interesado*" del RGPD establece:

"1. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida.

2. La comunicación al interesado contemplada en el apartado 1 del presente artículo describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 33, apartado 3, letras b), c) y d).

3. La comunicación al interesado a que se refiere el apartado 1 no será necesaria si se cumple alguna de las condiciones siguientes:

a) el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;

b) el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado a que se refiere el apartado 1;

c) suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.

4. Cuando el responsable todavía no haya comunicado al interesado la violación de la seguridad de los datos personales, la autoridad de control, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo haga o podrá decidir que se cumple alguna de las condiciones mencionadas en el apartado 3".

En el presente caso, la brecha entrañaba un alto riesgo para los derechos y libertades de las personas físicas. Según las manifestaciones que ha efectuado INSTITUTO MARQUÉS, ***(…)***.

(…).

En relación con la comunicación a los afectados, el artículo 34.1 del RGPD pone de manifiesto que dicha comunicación deberá comunicarse al interesado, sin dilación indebida. En este sentido, en el presente expediente no consta que la comunicación se hubiera realizado a todos los afectados que vieron expuestos sus datos personales, en la medida en que las manifestaciones de INSTITUTO MARQUÉS hacen referencia a que "*el subdirector general de INSTITUT MARQUES envió correos electrónicos a todas aquellas cuentas de correo de pacientes reales que se encontraban copiadas en dichas comunicaciones para informarles de lo sucedido*…". De esta afirmación se deduce claramente que la comunicación no se habría enviado a todas las personas que podrían haber visto sus datos personales expuestos.

Asimismo, la comunicación no se habría producido "sin la dilación indebida" que establece el artículo 34, en la medida en que se tiene constancia del ataque el día 21 de diciembre de 2021, y las posibles comunicaciones no comenzaron a realizarse hasta el día 25 de marzo de 2022, es decir, tres meses después de la constancia del ataque informático, sin que se justifique el motivo de tal dilación.

Por otro lado, el artículo 34.2 del RGPD se remite al artículo 33 del RGPD en relación con el contenido que debe tener esta comunicación. De este modo, el contenido es el recogido en el artículo 33 apartado 3, letras b), c) y d) RGPD, que establece:

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

b) comunicar el nombre y los datos 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 seguridad, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos."

En el presente supuesto, el contenido de los correos que INSTITUTO MARQUÉS ha enviado no se ajusta a lo dispuesto en el artículo 33 del RGPD en la medida en que han aportado una copia de tres de estos correos enviados en los que se puede apreciar que recogen ***(…)***, pero no recoge las exigencias previstas en el artículo 33.3 apartados b), c) y d) , y 34.2 del RGPD.

En el presente caso, la brecha entrañaba un alto riesgo para los derechos y libertades de las personas físicas, y no se han dado ninguna de las circunstancias enumeradas en el apartado 3 del artículo 34 del RGPD que eximiera a INSTITUTO MARQUÉS del deber de comunicar debidamente a los interesados que esta brecha se había producido.

De conformidad con las evidencias de las que se dispone en este acuerdo de inicio de 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 INSTITUTO MARQUÉS, por vulneración del artículo 34 del RGPD.

X

Tipificación y calificación de la infracción del artículo 34 del RGPD

De confirmarse, la citada infracción del artículo 34 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:

> *"(…)*
> *ñ) El incumplimiento del deber de comunicación al afectado de una violación de la seguridad de los datos que entrañe un alto riesgo para los derechos y libertades de los afectados, conforme a lo exigido por el artículo 34 del Reglamento (UE) 2016/679, salvo que resulte de aplicación lo previsto en el artículo 73 s) de esta ley orgánica. (…)"*

XI

Propuesta de sanción por la infracción del artículo 34 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 procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el artículo 83.2 del RGPD:

Como agravantes:

- La naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido (apartado a): Por no comunicar a los, al menos 400 afectados, que la brecha de seguridad en cuestión se había producido, y por no comunicar toda la información requerida por el artículo 34.2 RGPD, sin dilación indebida (entre el 21 de diciembre de 2021 y el 25 de marzo de 2022), a los afectados a los que sí se les realizó la citada comunicación.

- Las categorías de los datos de carácter personal afectados por la infracción (apartado g): En el presente supuesto, de acuerdo con la notificación de la entidad, se habrían visto comprometidos datos de origen racial, salud, genéticos, entre otros datos personales de los afectados.

Como atenuantes:

- Cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados (apartado c): se proporcionó información parcial o incompleta sobre la existencia de la brecha a algunos afectados.

Asimismo, se considera que procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el apartado 2 del artículo 76 "*Sanciones y medidas correctivas*" de la LOPDGDD:

- La vinculación de la actividad del infractor con la realización de tratamientos de datos personales (apartado b): se trata de una entidad habituada al tratamiento de datos personales de salud.

Como atenuantes:

- Disponer, cuando no fuere obligatorio, de un delegado de protección de datos (apartado g):

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 34 del RGPD, permite fijar inicialmente una sanción de 10.000 € (diez mil euros).

XII
Imposición 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, sin perjuicio 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.

Asimismo, las medidas que pudieran adoptarse en la resolución que ponga fin al procedimiento, serían de aplicación en todos los países de la Unión Europea en los que opere INSTITUTO MARQUÉS.

Se advierte que no atender a los requerimientos de este organismo podría 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 **INSTITUT MARQUÉS OBSTETRICIA I GINECOLOGIA, S.L.P.**, con NIF **B62187323**,

-por la presunta infracción del Artículo 5.1.f) del RGPD tipificada en el Artículo 83.5 del RGPD

-por la presunta infracción del Artículo 32 del RGPD tipificada en el Artículo 83.4 del RGPD,

-por la presunta infracción del Artículo 34 del RGPD tipificada en el Artículo 83.4 del RGPD

SEGUNDO: NOMBRAR como instructora a ***A.A.A.*** y, como secretaria, 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, la documentación procedente del IMI que ha dado lugar a las actuaciones previas de investigación, 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 y la documentación procedente del IMI sobre el proyecto de decisión.

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 sería:

- Por la supuesta infracción del artículo 5.1.f) del RGPD, tipificada en el artículo 83.5 de dicha norma, multa administrativa de cuantía 50.000,00 euros

- Por la supuesta infracción del artículo 32 del RGPD, tipificada en el artículo 83.4 de dicha norma, multa administrativa de cuantía 20.000,00 euros

- Por la supuesta infracción del artículo 34 del RGPD, tipificada en el artículo 83.4 de dicha norma, multa administrativa de cuantía 10.000,00 euros

QUINTO: NOTIFICAR el presente acuerdo a **INSTITUT MARQUÉS OBSTETRICIA I GINECOLOGIA, S.L.P.**, con NIF **B62187323**, 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 procedimiento 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 64.000,00 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 64.000,00 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 48.000,00 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 (64.000,00 euros o 48.000,00 euros), deberá hacerlo efectivo mediante su ingreso en la cuenta nº ***IBAN: ES00-0000-0000-0000-0000-0000*** 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 se producirá su caducidad y, en consecuencia, el archivo de actuaciones; de conformidad con lo establecido en el artículo 64 de la LOPDGDD.

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.

935-030423

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

>>

SEGUNDO**:** En fecha 18 de octubre de 2023, la parte reclamada ha procedido al pago de la sanción en la cuantía de **48000 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 **EXP202204816**, de conformidad con lo establecido en el artículo 85 de la LPACAP.

SEGUNDO: NOTIFICAR la presente resolución a ***INSTITUT MARQUÉS OBSTETRICIA I GINECOLOGIA, 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