- **Expediente Nº: EXP202205755**

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 12 de julio de 2023, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a ***ROAMS TIC, S.L.*** (en adelante, la parte reclamada), mediante el Acuerdo que se transcribe:

<<

Expediente N.º: EXP202205755

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: Durante el período comprendido entre el 16/05/2022 y el 30/09/2022, tuvieron entrada en esta Agencia ocho reclamaciones interpuestas por ***A.A.A.*** (parte reclamante 1), ***B.B.B.*** (parte reclamante 2), ***C.C.C.*** (parte reclamante 3), ***D.D.D.*** (parte reclamante 4), ***E.E.E.*** (parte reclamante 5), ***F.F.F.*** (parte reclamante 6), ***G.G.G.*** (parte reclamante 7) ***y H.H.H.*** (parte reclamante 8), respectivamente. Las reclamaciones se dirigen contra la entidad ROAMS TIC, S.L., con NIF ***B34263582*** (en adelante, la parte reclamada, entidad reclamada o ROAMS TIC). Los motivos en que basan la reclamación son los siguientes:

Las partes reclamantes comunican a la AEPD la recepción de un correo electrónico, desde la dirección ***"***EMAIL.1"***, en el que presuntos hackers avisan ***(…)***. Dichas comunicaciones, que son recibidas por las partes reclamantes en fechas 14 y 15/05/2022, *están firmadas por* ***"I.I.I." y "J.J.J.".***

La parte reclamante 2 señala que nunca ha accedido a la web de la entidad reclamada.

La parte reclamante 5 solicita en su reclamación que la parte reclamada, a la que dice desconocer, suprima todos sus datos personales, señalando al respecto que

desconoce cómo han llegado tales datos a poder de la entidad reclamada.

La parte reclamante 6 formula su reclamación con motivo del correo recibido de la parte reclamada, de fecha 24/06/2022, ***(…)***. En esta reclamación se reproduce el texto del correo electrónico citado:

(…)

La parte reclamante 7 también da cuenta de la recepción del mismo correo electrónico remitido por la entidad reclamada en fecha 25/06/2022.

La parte reclamante 8 manifiesta que tuvo conocimiento de que la parte reclamada disponía de su dirección de correo electrónico mediante la comunicación que dicha entidad le remitió informando sobre un incidente de seguridad. Con ese motivo, con fecha 02/07/2022 ejercitó su derecho de acceso para conocer los datos personales que estaban disponibles en dicha entidad y su origen, recibiendo respuesta en la que figuraba su dirección de correo, pero asociada a un nombre, apellido y fecha de nacimiento que no le corresponden. Insistió ante la parte reclamada para recibir información sobre el origen de sus datos personales y le respondieron que no había acreditado que la dirección de correo sea de la parte reclamante 8.

Con las reclamaciones se aportaron los documentos siguientes:

1. (…).

(…):

(…)

En la misma comunicación electrónica se indica una nueva dirección, que sustituirá a la anterior, para facilitar más información y/o pruebas a los destinatarios (…).

2. ***(…).***

3. La parte reclamante 8 aportó la solicitud de acceso a los datos personales formulada ante la parte reclamada y la respuesta facilitada por esta entidad, en la que se informa sobre los datos que constan en sus sistemas, los fines de tratamiento, los destinatarios y el plazo de conservación.

SEGUNDO: Con fecha 18/05/2022, se notificó a la División de Innovación Tecnológica de esta Agencia una brecha de seguridad de los datos personales por parte de la entidad ROAMS TIC, como responsable del tratamiento.

En el escrito recibido se informa ***(…).***

(…).

TERCERO: De conformidad con el artículo 65.4 de la Ley Orgánica 3/2018, de 5 de

diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD), recibidas las primeras reclamaciones, se dio cuenta a la parte reclamada de las reclamaciones recibidas, adjuntándole copia del correo electrónico aportado por las partes reclamantes, para que procediese a su análisis e informase a esta Agencia en el plazo de un mes, de las acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos.

El traslado, que se practicó conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), fue recogido en fecha 06/06/2022 como consta en el acuse de recibo que obra en el expediente.

El plazo otorgado a ROAMS TIC transcurrió sin que se recibiese respuesta al escrito de traslado.

CUARTO: Con fecha 27/06/2022, la parte reclamada presentó una nueva notificación de brecha de seguridad dirigida a la División de Innovación Tecnológica de esta Agencia.

En el escrito presentado se informa ***(…).***

(…):

. (…).
. (…).

QUINTO: Con fecha 11/11/2022, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la parte reclamante 8.

CUARTO: 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:

1. Como “Antecedentes”, en el Informe de Actuaciones Previas de Investigación se destaca lo siguiente.

(…).
(…).
(…).
(…).

2. En la información obtenida en ASEXOR, la empresa reclamada es una sociedad española dedicada a la prestación de servicios relacionados con las tecnologías de la información y la informática. ***(…)***. Consta, asimismo, que su volumen de ventas en 2021 ascendió a ******CANTIDAD.1***.

3. Tal y como consta en la web ***"***WEB.1", (…).***

4. ***(…)***

5. Con fecha 02/12/2022 se remite requerimiento de información a la entidad reclamada. De la respuesta recibida se desprende:

Origen de los datos de la Base de Datos de Clientes

(…)

Descripción de los hechos

La entidad ha remitido nuevamente el informe aportado con la segunda notificación de brecha. En dicho informe figura:

. (…)

. (…).
(…).

. (…).

. (…).

Causa de la brecha

(…).

Comunicación a los afectados

(…).

Respecto del encargado del tratamiento

(…).

Respecto de las medidas de seguridad implantadas

. (…).

. (…).

. (…).

. (…).

. (…).

. (…):

. (…).
(…).

Información sobre la recurrencia de estos hechos y número de eventos análogos acontecidos en el tiempo.

La entidad manifiesta que no se conoce ni se han registrado hechos similares a los acontecidos.

FUNDAMENTOS DE DERECHO

I
Competencia

De acuerdo con los poderes que el artículo 58.2 del RGPD, otorga a cada autoridad de control y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 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

ROAMS TIC Es una empresa con forma jurídica de sociedad limitada dedicada a la prestación de servicios relacionados con las tecnologías de la información y la informática. Dispone de una ***(…).***

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:

"responsable del tratamiento" o "responsable": la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros".

Se considera persona física identificable aquella cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

Asimismo, debe entenderse por tratamiento "*cualquier operación o conjunto de*

operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción".

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 indicadas en los Antecedentes, categorizada como una brecha de confidencialidad, provocada por una vulnerabilidad de la web que permitió el acceso y exfiltrado de datos de la base de datos de clientes de dicha web.

Como resultado de estos hechos, se han visto comprometidos los datos básicos y de contacto (nombre, apellidos, dirección de correo electrónico y teléfono) de ***(…)***.

Según el GT29 se produce una "Violación de la confidencialidad" cuando se produce una revelación no autorizada o accidental de los datos personales, o el acceso a los mismos.

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 el artículo 32 del RGPD, que reglamentan la seguridad del tratamiento.

III
Artículo 5.1.f) del RGPD

El artículo 5 del RGPD establece los principios que han de regir el tratamiento de los datos personales y menciona, entre ellos, el de *"integridad y confidencialidad"*:

"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 relación con este principio, el Considerando 39 del referido RGPD señala que:

"[…]Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento".

Teniendo en cuenta los hechos antes indicados, de los que es presuntamente

responsable la parte reclamada, se considera que existen indicios suficientes, sin perjuicio de lo que resulte de la instrucción, sobre una posible vulneración del principio de confidencialidad establecido en el artículo 5.1.f) del RGPD, *"principios relativos al tratamiento"*, toda vez que, a raíz de la brecha de confidencialidad, los datos personales *de **(…)*** obrantes en su base de datos de clientes resultaron indebidamente expuestos a terceros. ***(…)***.

Este deber de confidencialidad tiene como finalidad evitar que se realicen filtraciones de los datos personales no consentidas por sus titulares.

IV
Obligación incumplida. 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 artículo 32 no establece medidas de seguridad estáticas, sino que corresponderá a responsables y encargados determinar aquellas medidas de seguridad que son necesarias para garantizar la confidencialidad, la integridad y la disponibilidad de los datos personales, por lo tanto, un mismo tratamiento de datos puede implicar medidas de seguridad distintas en función de las especificidades concretas en las que tiene

lugar dicho tratamiento de datos.

En consonancia con estas previsiones, el Considerando 75 del RGPD establece:

"(75) Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados".

Asimismo, el Considerando 83 del RGPD establece:

"(83) A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como 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, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales".

En definitiva, el primer paso para determinar las medidas de seguridad será la evaluación del riesgo. Una vez evaluado será necesario determinar las medidas de seguridad encaminadas para reducir o eliminar los riesgos para el tratamiento de los datos.

La seguridad de los datos requiere la aplicación de medidas técnicas u organizativas apropiadas al tratamiento de los datos personales para proteger dichos datos contra el acceso, uso, modificación, difusión, pérdida, destrucción o daño accidental, no autorizado o ilícito. En este sentido, las medidas de seguridad son claves a la hora de garantizar el derecho fundamental a la protección de datos. No es posible la existencia del derecho fundamental a la protección de datos personales si no es posible garantizar la confidencialidad, la integridad y la disponibilidad de estos.

No debe olvidarse que, de conformidad con el artículo 32.1 del RGPD citado, las medidas técnicas y organizativas a aplicar para garantizar un nivel de seguridad adecuado al riesgo deben tener en cuenta el estado de la técnica, los costes de

aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas.

Derivado de la actividad a la que se dedica, la parte reclamada está obligada a realizar de forma muy especializada un análisis de los riesgos y una implantación de medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo de su actividad para los derechos y libertades de las personas.

Por tanto, la parte reclamada, a la hora de evaluar los riesgos y determinar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo para los derechos y libertades de las personas físicas de los tratamientos de datos que realiza, está obligada a tener en cuenta la concreta actividad que supone su negocio, que conlleva tratar datos personales de forma continua y a gran escala (numerosos datos a recoger, procesar, almacenar…); la tipología de datos tratados: entre ellos, datos identificativos, de contacto, los relativos a DNI y fecha de nacimiento, ingresos y datos financieros; o el contexto: existencia de aplicativos web en internet, es decir, en un entorno no aislado, lo que conlleva riesgos derivados de la propia interconectividad que supone la red, los cuales deben atenderse de forma especializada.

(…).

(…).

(…).

(…).

(…).

(…).

Todo lo expuesto demuestra que la parte reclamada no contaba con las medidas de seguridad apropiadas para garantizar que no se produjera el incidente de seguridad como el que tuvo lugar en el presente caso, es decir, no aplicó medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo de sus tratamientos de datos personales, con la consiguiente falta de diligencia de la parte reclamada, en tanto que entidad responsable, a la hora de evitar el acceso no autorizado por terceros ajenos.

Prueba de que los sistemas de información de la parte reclamada no contaban con las medidas adecuadas son las medidas adoptadas con motivo del incidente de seguridad constatado, entre las que figuran algunas que se consideran básicas para garantizar la seguridad de los datos personales, como son la implantación de un ***(…).***

Por tanto, de conformidad con las evidencias de las que se dispone en este momento de 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 la parte reclamada, por vulneración del artículo 32 del RGPD.

V
Tipificación y calificación de las infracciones

El incumplimiento de lo establecido en el artículo 5.1.f) del RGPD supone la comisión de una infracción tipificada en el apartado 5.a) del artículo 83 del RGPD, que bajo la rúbrica *"Condiciones generales para la imposición de multas administrativas"* dispone lo siguiente:

"5. 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".

Por su parte, la LOPDGDD en su artículo 71, Infracciones, señala 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 de la LOPDGDD indica:

"Artículo 72. Infracciones consideradas muy graves.
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".

Por otra parte, la vulneración del artículo 32 del RGPD se encuentra tipificada en el artículo 83.4.a) del citado RGPD en los siguientes términos:

"4. 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.
(…)".

Y el artículo 73 de la LOPDGDD, a efectos de prescripción, califica de *"Infracciones consideradas graves"*:

"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".
(…)".

VI
Poderes correctivos

Para el caso de que concurra una infracción de los preceptos del RGPD, entre los poderes correctivos de los que dispone la Agencia Española de Protección de Datos, como autoridad de control, el artículo 58.2 de dicho Reglamento contempla los siguientes:

"2 Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:
(…)
b) dirigir a todo responsable o encargado del tratamiento un apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento;"
(...)
d) ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado;
(…)
i) imponer una multa administrativa con arreglo al artículo 83, además o en lugar de las medidas mencionadas en el presente apartado, según las circunstancias de cada caso particular;".

Según lo dispuesto en el artículo 83.2 del RGPD, la medida prevista en la letra d) anterior es compatible con la sanción consistente en multa administrativa.

VII
Propuesta de sanción

Con respecto a las infracciones de los artículos 32 y 5.1.f) del RGPD, atendiendo a los hechos expuestos y sin perjuicio de lo que resulte de la instrucción del procedimiento, se considera que la sanción que correspondería imponer es de multa administrativa.

A fin de determinar la multa administrativa a imponer se han de observar las previsiones de los artículos 83.1 y 83.2 del RGPD, preceptos que señalan**:**

"1. Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 9 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias.

2. Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:
a) 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;
b) la intencionalidad o negligencia en la infracción;

c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;
d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;
e) toda infracción anterior cometida por el responsable o el encargado del tratamiento;
f) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;
g) las categorías de los datos de carácter personal afectados por la infracción;
h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida;
i) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;
j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42, y
k) 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".

Por su parte, el artículo 76 "*Sanciones y medidas correctivas" de la LOPDGDD* dispone:

"1. Las sanciones previstas en los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679 se aplicarán teniendo en cuenta los criterios de graduación establecidos en el apartado 2 del citado artículo.
2. De acuerdo a lo previsto en el artículo 83.2.k) del Reglamento (UE) 2016/679 también podrán tenerse en cuenta:

a) El carácter continuado de la infracción.
b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.
c) Los beneficios obtenidos como consecuencia de la comisión de la infracción.
d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.
e) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.
f) La afectación a los derechos de los menores.
g) Disponer, cuando no fuere obligatorio, de un delegado de protección de datos.
h) El sometimiento por parte del responsable o encargado, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier interesado".

En este caso, considerando la gravedad de las infracciones constatadas, atendiendo especialmente al volumen de datos personales implicados en la incidencia constatada, procede la imposición de multa, además de la adopción de medidas, en su caso.

La multa que se imponga deberá ser, en cada caso individual, efectiva, proporcionada y disuasoria, conforme a lo establecido en el artículo 83.1 del RGPD. Así, se considera, con carácter previo, la condición de pequeña empresa y el volumen de negocio de la parte reclamada (**...**).

De acuerdo con los preceptos indicados, 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 del procedimiento, a efectos de fijar el

importe de las sanciones a imponer en el presente caso, se considera que procede graduar las sanciones de acuerdo con los siguientes criterios que establecen los preceptos transcritos:

1. Infracción del artículo 5.1.f) del RGPD, tipificada en el artículo 83.5.a) del citado Reglamento, y calificada como muy grave a efectos de prescripción en el artículo 72.1.a) de la LOPDGDD:

En una valoración inicial, se estiman concurrentes como agravantes los criterios de graduación siguientes:

. Artículo 83.2.a) del RGPD: *"a) 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".*

× Se considera que la naturaleza de la infracción es grave puesto que ha acarreado una pérdida de confidencialidad y, por tanto, de disposición y control irremediable sobre los datos personales, ***(…)***.

. En relación con la duración de la infracción, ***(…)***.

× Número de interesados afectados asciende a ***(…)*** usuarios de la web de la entidad reclamada.

. La naturaleza de los perjuicios causados a las personas interesadas, que han visto incrementado el riesgo en su privacidad, por cuanto perdieron todo el control sobre sus datos personales, lo que supone riesgo alto de uso fraudulento, vaciando así de contenido el derecho fundamental a la protección de datos personales que, como indica el Tribunal Constitucional, persigue garantizar a la persona un poder de control y disposición sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado.

. Artículo 83.2.b) del RGPD: *"b) la intencionalidad o negligencia en la infracción"*.

En este supuesto la negligencia de la parte reclamada en el cumplimiento y observancia de las medidas técnicas y organizativas para garantizar la seguridad necesaria para la protección de los datos personales, concretamente para garantizar la confidencialidad de estos debe calificarse de "grave", por cuanto no había dispuesto las medidas de seguridad pertinentes a pesar de que el incidente tiene causa en una vulnerabilidad conocida públicamente.

A este respecto, se tiene en cuenta lo declarado en Sentencia de la Audiencia Nacional de 17/10/2007 (rec. 63/2006) que, partiendo de que se trata de entidades cuya actividad lleva aparejado en continuo tratamiento de datos, indica que *"…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".

La parte reclamada realiza tratamientos de datos personales relativos a la salud de manera sistemática y debe extremar el cuidado en el cumplimiento de sus obligaciones en la protección de los mismos.

Entiende esta Agencia que la diligencia tiene que deducirse de hechos concluyentes, que consten debidamente acreditados y directamente relacionados con los elementos que configuran la infracción, de tal modo que pueda deducirse que la misma se ha producido a pesar de todos los medios dispuestos por el responsable para evitarla. En este caso, la actuación de la parte denunciada no tiene este carácter.

. Artículo 76.2.b) de la LOPDGDD: *"b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales".*

La alta vinculación de la actividad de la parte reclamada con la realización de tratamientos de datos personales, considerando la actividad que desarrolla.

Considerando los factores expuestos, la valoración inicial que alcanza la multa, por la infracción del artículo 5.1.f) del RGPD, es de 30.000 euros (treinta mil euros).

2. Infracción del artículo 32 del RGPD, tipificada en el 83.4.a) del citado RGPD, y calificada como grave a efectos de prescripción en el artículo 73.f) del RGPD:

En una valoración inicial, se estiman concurrentes como agravantes los mismos criterios de graduación señalados en el apartado anterior.

Considerando los factores expuestos, la valoración inicial que alcanza la multa, por la infracción del artículo 32 del RGPD, es de 20.000 euros (veinte mil euros).

VIII
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.

En tal caso, en la resolución que se adopte, esta Agencia podrá requerir a la entidad responsable para que, en el plazo que se determine, adecúe su actuación a la normativa de protección de datos personales, con el alcance expresado en los Fundamentos de Derecho del presente acuerdo y sin perjuicio de lo que resulte de la

instrucción.

No obstante, a este respecto, se tiene en cuenta que la parte reclamada ha manifestado que ***(…)***.

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 ROAMS TIC, S.L., con NIF ***B34263582***, por las presuntas infracciones siguientes:

- por la presunta infracción del artículo 5.1.f) del RGPD, tipificada conforme a lo dispuesto en el artículo 83.5 del RGPD, calificada como muy grave a efectos de prescripción en el artículo 72.1.a) de la LOPDGDD.

- por la presunta infracción del artículo 32 del RGPD, tipificada conforme a lo dispuesto en el artículo 83.4 del RGPD, calificada como grave a efectos de prescripción en el artículo 73.f) de la LOPDGDD.

SEGUNDO: NOMBRAR como instructor a ***K.K.K.*** y secretario a ***L.L.L.***, 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, las reclamaciones interpuestas por las partes reclamantes y su documentación, 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 de:

. Por la presunta infracción del artículo 5.1.f) del RGPD, tipificada en el artículo 83.5.a) del mismo Reglamente, una sanción por importe de 30.000 euros (treinta mil euros).

. Por la presunta infracción del artículo 32 del RGPD, tipificada en el artículo 83.4.a) del mismo Reglamente, una sanción por importe de 20.000 euros (veinte mil euros).

QUINTO: NOTIFICAR el presente acuerdo a ROAMS TIC, S.L., con NIF ***B34263582***, 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 40.000 euros (cuarenta mil 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 40.000 euros (cuarenta mil 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 30.000 euros (treinta mil 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 (40.000 euros o 30.000 euros), deberá hacerlo efectivo mediante su ingreso en la cuenta nº ***IBAN: ES00-0000-0000-0000-0000-0000 (BIC/Código SWIFT: CAIXESBBXXX)*** 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.

935-290523

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

>>

SEGUNDO**:** En fecha 21 de julio de 2023, la parte reclamada ha procedido al pago de la sanción en la cuantía de **30000 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.

CUARTO: En el citado Acuerdo de inicio transcrito anteriormente, se señalaba que 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…".*

Habiéndose recibido escrito mediante el que ***ROAMS TIC, S.L.*** informa que ha adoptado las medidas necesarias para que no se vuelvan a producir los hechos determinantes de la infracción cometida, por parte de esta Agencia se acusa recibo del mismo, sin que esta declaración suponga ningún pronunciamiento sobre la regularidad o licitud de las medidas adoptadas.

Se advierte sobre lo dispuesto en el artículo 5.2 del RGPD, que establece el principio de responsabilidad proactiva cuando señala que "*El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo*". Este principio hace referencia a la obligación que recae en el responsable del tratamiento no solo de diseñar, implementar y observar las medidas jurídicas, técnicas y organizativas adecuadas para que el tratamiento de datos sea acorde con la normativa, sino de permanecer activamente atento a lo largo de todo el ciclo de vida del tratamiento para que ese cumplimiento sea correcto, siendo además capaz de demostrarlo.

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 **EXP202205755**, de conformidad con lo establecido en el artículo 85 de la LPACAP.

SEGUNDO: NOTIFICAR la presente resolución a ***ROAMS TIC, S.L.***.

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.

1219-181022

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